Witness Name: Emran Mian

Statement No.: 3

Exhibits: EM8/01 – EM8/57

Dated: 23 July 2025

UK COVID-19 INQUIRY

WITNESS STATEMENT OF
EMRAN MIAN

Contents

I, Emran Mian, will say as follows:

Section A - Introduction

1. On 2 July 2025 I became the Permanent Secretary of the Department of Science, Innovation and Technology (**"DSIT"**). Previously, from 17 July 2023, I had been a Director General in DSIT with responsibility for the Digital, Technology and Telecoms Group. I replaced Susannah Storey, who had been the Director General since August 2019. Prior to joining DSIT, I was the Director General for Decentralisation and Local Growth within the Department for Levelling Up, Housing and Communities and was in this role at the start of the pandemic.

2. This statement is provided in response to the requests from the Chair of the Inquiry for a statement which covers the relevant issues raised in the Provisional Outline of Scope for Module 8 of the Covid-19 Inquiry. I understand that Module 8 is focused on the impact of the pandemic on children and young people across the UK.

3. This statement responds to the sections of the Inquiry's request dated 24 October 2024 relevant to DSIT (M08-DCMS-001) and the whole of the Inquiry's request dated 24 February 2025 (M08-DCMS-002) and 25 February 2025 (M08-DSIT-001) **("the Rule 9 Requests")**. The subject of all these requests is online safety policy, covering a period from prior to the pandemic to the present day, with a specific focus on children and young people.

4. As the Inquiry is interested in online safety policy over a prolonged period of time, my statement is split into three time periods: pre-pandemic, the pandemic and post-pandemic. Within each of those time periods my statement looks at the issues of mis and disinformation and media literacy, as well as online safety.

5. I previously submitted a statement for Module 4 **[EM8/01 - INQ000474308]**, which was focused on DSIT's work to tackle online mis and disinformation. In the expectation that this statement will be treated as a standalone document, I quote or paraphrase from the Module 4 statement where applicable. This statement addresses the work which

both the Department for Digital, Culture, Media and Sport ("**DCMS**") and DSIT undertook in relation to online harms policy.

6. Whilst I have a degree of personal recollection of some of the events or processes described in this witness statement, I have also co-ordinated and consulted with colleagues across DSIT who have knowledge and experience of matters covered in this statement. Their contributions have been used to respond to the Rule 9 Requests. 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.

Section B - Roles and responsibilities of DSIT

7. Prior to February 2023, DCMS was responsible for a large amount of digital policy across government including telecommunications and digital infrastructure, digital and tech policy, online harms and security, the cyber and AI sectors, and data infrastructure.

8. 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 the newly created DSIT. The formal transfer of responsibilities from DCMS to DSIT occurred on 3 May 2023 in accordance with the transfer of functions order **[EM8/02 - INQ000361212]**. 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.

9. DSIT has a wide remit and is responsible for policy in a number of areas including AI, scientific research and development, space, cyber security, digital infrastructure, the Government Digital Service (**"GDS"**), as well as online safety. GDS was officially transferred to DSIT on 24th July 2024, with a transfer of functions order expected in June 2025. Since the announcement, DSIT has administratively handled GDS, with the Secretary of State responsible for it from July 2024.

10. DSIT has overall primary responsibility for online safety policy, including where it specifically relates to children. It is therefore responsible for policies including mis and

disinformation and media literacy in addition to having responsibility the development of online safety regulatory policy. However, there are specific areas where responsibility is held by other government departments. For example, responsibility for online child sexual exploitation is the responsibility of the Home Office ("**HO"**), policy relating to accessing online educational and social development tools is the responsibility of the Department for Education ("**DfE"**), and policies concerning the mental health and wellbeing of children is the responsibility of the Department of Health and Social Care ("**DHSC"**). Responsibility for these areas is devolved under all three settlements. These departments generally hold responsibility in England only, while devolved governments manage these responsibilities in other parts of the UK.

11. This statement covers three main policy areas: mis and disinformation, media literacy and online safety. Both mis and disinformation and media literacy policy are devolved matters; however, internet services policy is reserved across the United Kingdom. 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. The Online Safety Act 2023 ("**the Act"**) **[EM8/03 - INQ000642745]** sets out comprehensive measures to protect children online, and these are enforced by Ofcom across the entire UK. The Act also legislates for a number of new offences, as will be explained in more detail below. The territorial extent of these offences varies; they do not all apply across the whole UK. Devolved governments in Scotland, Wales, and Northern Ireland can also implement complementary policies and initiatives to support online safety within their regions and devolved competences. These might include educational programs, local enforcement strategies and community support services.

12. When I was the Director General of the Digital, Technology and Telecoms Group, I had responsibility for a number of directorates. One of those was the Security and Online Harms Directorate, whose remit covers policy relating to online safety, security and mis and disinformation. This means that I had responsibility for the following key staff members who worked in this policy area:

    a) Director of Security and Online Harms (SCS2) who leads the Security and Online Harms Directorate and is responsible for its work.

b) Deputy Director Policy and Regulation (SCS1) who oversees the teams working on online safety policy and regulation, including implementation of the Online Safety Act.

c) Deputy Director Strategy and Analysis (SCS1) who oversees the analytical team and teams working on wider safety technologies and strategy.

d) Deputy Director Information Resilience and Public Safety (SCS1), who oversees the teams working on mis and disinformation policy, media literacy and the operational response to mis and disinformation during public safety incidents.

e) Deputy Director Information Threats and Security (SCS1) who oversees the analytical and technology team who support operational incidents, and the operational response to mis and disinformation which relates to national security.

13. Prior to the pandemic, the Secretary of State was Sir Jeremy Wright KC, who was in post from 9 July 2018 to 24 July 2019, when he was replaced by Nicky Morgan (now Baroness Morgan of Cotes) who was in post from 24 July 2019 to 13 February 2020. During this period, the relevant junior ministers were Margot James who was in post from 9 January 2018 to 18 July 2019 and Matt Warman who was in post from 24 July 2019 to 13 February 2020.

14. The DCMS Secretary of State during the majority of the pandemic was Oliver Dowden, who was in post from 13 February 2020 to 15 September 2021, when Nadine Dorries succeeded him. The junior minister who had responsibility and oversight of online safety policy during the pandemic was Caroline Dinenage, who was in post from 13 February 2020 to 15 September 2021, when Chris Philp succeeded her.

15. In the post pandemic period, Nadine Dorries was replaced by Michelle Donelan on 6 September 2022. Following the machinery of government changes in February 2023, Michelle Donelan became DSIT's Secretary of State and remained in post (apart from a brief period of maternity leave) until 5 July 2024 when, following the general election, the present incumbent Peter Kyle was appointed. During this period the relevant junior ministers were Chris Philp who remained in post until 7 July 2022, Damian Collins who

was in post until 27 October 2022, Paul Scully who remained in post until 13 November 2023, and Saqib Bhatti who was in post until 5 July 2024, when he was replaced by the present incumbent Baroness Jones of Whitchurch.

16. As set out further below in Section C, DCMS worked in collaboration with the HO to undertake an online harms consultation in 2019. This work evolved to the development of the Online Safety Bill (**"the Bill"**) and later the Act **[EM8/03 - INQ000642745]**, led by DCMS (and now DSIT), which I discuss further below.

17. As detailed in Section C, DCMS gave significant thought to children and young people in its work to tackle online harms during the pandemic, including through the development of the Bill and later the Act. This work had started prior to the pandemic with the 2019 Online Safety White Paper (**"the White Paper"**).

Section C - Pre-pandemic (1 January 2015 to 31 December 2019)

Work to understand patterns of online behaviour

18. Prior to the pandemic, DCMS commissioned the UK Council for Child Internet Safety **[EM8/04 - INQ000182264]** and referenced the child safety review in the Internet Safety Strategy Green Paper (**"the Green Paper"**) **[EM8/05 - INQ000598414]**, as detailed in paragraph 28 below. Additionally, DCMS relied on public consultations, external research, and reports to understand the online environment and the use of social media. As set out below, this work fed into DCMS' work to create a legislative and regulatory framework which would protect UK citizens when online. DCMS' focus was the creation of that framework, rather than the identification or monitoring of specific online harms. DCMS did not have the remit to monitor social media for harmful online content, except in the specific case of online mis and disinformation where a team could be 'stood up' at times when there was heightened risk to either public safety or national security, such as an election, as is explained further later in my statement. This is because DCMS had policy responsibility for that specific type of online harm. It is my understanding that at the time no government department or agency had responsibility for monitoring legal but harmful online content in general. It would not have been feasible for government to have such a remit, as millions of pieces of content are posted on social media each day and the resource needed would be vast.

One statistic which provides some context as to the scale of the problem is that in the third quarter of 2018, Facebook reported removing 8.7 million pieces of content globally for breach of its child nudity and sexual exploitation policies. While this is a global figure, content published internationally is available within the UK, indeed, this proliferation of harmful content was, one of the key issues the Act sought to address.

19. DCMS therefore gained its knowledge of the information environment and the types of harmful content which were available online from external publicly available sources such as reporting from Ofcom and the Information Commissioner's Office **("the ICO**"), alongside information which was obtained from meeting industry stakeholders, including civil society organisations and academia, and from colleagues across government. Widescale government monitoring of social media posts would have had implications in relation to the public's right to freedom of expression and their privacy rights. There would also be practical issues which prevented government from monitoring all social media activity to identify harmful but legal content produced in the UK. Firstly, it is not always possible to identify the geographic location from where a post has been made. Secondly, government would be unable to access any posts which were made within private or closed groups.

20. Prior to the pandemic, DCMS was aware that the existing, fragmented regulatory regime needed reform and was reliant upon platforms having their own measures in place to address content harmful to children, such as robust terms of service which prevented harmful content being available, and the platforms enforcing those terms of service. In the absence of a legislative framework, where platforms would be answerable to an independent regulator, government had very few levers which it could use to encourage platforms to remove content that is harmful to children, meaning that it was reliant upon the industry working in close partnership with it in order to deliver any online safety initiatives. The position was different in relation to illegal content, which at the time was governed by the European e-Commerce Directive, as implemented into domestic law. This directive made consistent the position that providers of platforms were liable for content they host under the criminal or civil law once they become aware of it on their sites. However, providers did not have legal responsibility for content they did not have knowledge of.

21. In October 2017, the government published the Green Paper, with the consultation on its contents running to December 2017 **[EM8/05 - INQ000598414]**. This was because the government had recognised that as the internet had developed, so had online risks and that there were types of behaviour which were being condoned or seen as acceptable online, which would not be acceptable outside the online environment. DCMS was the lead department for the Green Paper, and the strategy as a whole. However, as acknowledged in the Green Paper, there were a wide range of partners across government with an interest in online safety, including the HO, DfE, DHSC and The Ministry of Justice. The Green Paper and consultation considered various aspects of online safety including:

    a) the introduction of a social media code of practice, transparency reporting and a social media levy
    b) technological solutions to online harms
    c) developing children's digital literacy
    d) support for parents and carers
    e) adults' experience of online abuse and
    f) young people's use of online dating websites/ applications

22. Subsequently, in April 2019 the government published the White Paper, which set out the intention to establish "*a new regulatory framework to improve our citizens' safety online"* **[EM8/06 - INQ000610032]**. As set out in the White Paper, the objectives of the proposed regulatory 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.

23. The White Paper, 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 2018 Report"**) 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.' **[EM8/07 - INQ000615302].**

24. 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 **[EM8/08 - INQ000610021]**.

25. The 2018 Report also provided data on the specific online services which children were using, although this was not specifically mentioned in the White Paper **[EM8/07 - INQ000615302]**. The 2018 Report found 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 **[EM8/07 - INQ000615302]**.

26. 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, could be used a tool for abuse and bullying and used to undermine civil discourse. It referred to the following evidence from the Ofcom and ICO joint 2018 Internet users' experience of harm online: summary of survey research report: *'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'* **[EM8/06 - INQ000610032], [EM8/09 - INQ000610023]**.

27. 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 in the White Paper, such as Facebook's 2018 transparency report, which reported removing over 14 million pieces of content related to terrorism or violent extremism in 2018.

28. Nevertheless, the White Paper acknowledged that '*most children have a positive experience online*' **[EM8/06 - INQ000610032]**. The White Paper found 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 the UK Council for Child Internet Safety (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 **[EM8/09 - INQ000361191]**.

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 **[EM8/10 - INQ000610018]**.

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 **[EM8/11 - INQ000610020]**. The 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.

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

[EM8/07 - INQ000615302] 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.

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 **[EM8/12 - INQ000610019]**. 43 per cent said 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.

29. As mentioned above, DCMS' focus at this time, in relation to online safety, was to create a regulatory framework which would help to keep the public safe online. It did not conduct any work on children and young people's online safety in the context of emergency preparedness and resilience, or more specifically pandemic planning. The work which DCMS had undertaken across its policy portfolio in relation to pre-pandemic planning was covered in more detail in DCMS' Module 1 statement.

Misinformation/disinformation

30. Government began to consider mis and disinformation in 2017, when it produced the Green Paper. However, it was not until March 2018, following an incident in Salisbury, where the nerve agent Novichok had been used in the attempted assassination of Segei and Yulia Skripal, that a policy team was established in DCMS. Following that incident, there had been an increase in Russian disinformation attempting to deny any Russian involvement.

31. In May 2018, the government responded to the Green Paper, setting out its intention to manage new and emerging issues, including disinformation **[EM8/13 - INQ000102740]**. In relation to mis and disinformation, the government aimed to prevent misleading information from being disseminated for political, personal, and/or financial gain. In August 2018, cross government discussions, led by the Cabinet Office

("**CO**"), took place to develop a counter disinformation strategy **[EM8/14 - INQ000102749]**.

32. The increasing risks in this area, including concerns over how mis and disinformation could impact UK elections, led the government to consider establishing a Counter Disinformation Cell ("**the CDC**") in 2019. DCMS identified key cross-government stakeholders – the Foreign, Commonwealth and Development Office **(FCDO)**, CO and HO - with a view to forming what would become the CDC (and later the Counter Disinformation Unit ("**the CDU**")). This structure was intended to provide government with the most comprehensive picture possible about the level, scope, and impact of disinformation during times of heightened risk. An early official draft outlined the rationale for this and identified the key stakeholders and teams **[EM8/15 - INQ000361183]**.

33. On 7 February 2019, DCMS chaired a disinformation roundtable with the relevant government stakeholders referred to above, to discuss the potential structure and make-up of the CDC **[EM8/16 - INQ000102753]**. Due to government concern over the potential of mis and disinformation to manipulate elections, an illustrative general election scenario was used at this meeting to test the CDC's proposed structure. Additionally, there was a discussion about establishing working relationships with social media platforms. On 15 February 2019, a DCMS official chaired a second disinformation roundtable discussion, which focused on developing the cross-government response structure.

34. On 20 February 2019, a submission was put to the DCMS Minister for Digital and Creative Industries setting out DCMS' preferred approach to how the proposed CDC would respond to disinformation, particularly in periods of heightened risk **[EM8/17 - INQ000102799]**. The intention was to strengthen the government's capability in this area through three work streams: a) cross-Whitehall coordination of operational capabilities b) cross-Whitehall collaboration with major social media platforms and c) strengthening public resilience.

35. On 25 February 2019, there was a third disinformation roundtable in which government stakeholders continued to discuss the CDC's structure.

36. DCMS formally established the CDC in March 2019, after Downing Street wrote to departments setting out the Prime Minister's position on ministerial responsibilities for countering disinformation **[EM8/18 - INQ000102807]**. While this strategy was a cross-government effort, the DCMS Secretary of State was tasked with leading on overall counter disinformation policy:

> *"The Culture Secretary will formally lead on HMG's overall counter disinformation policy in order to provide a single spokesperson to set out the Government's position and coordinate the delivery of the disinformation strategy. This role includes setting the direction, focus and principles of domestic policy; leading our engagement with social media companies and the media; working with partners to further the aims of the strategy and representing and promoting domestic activity amongst our international partners and the public. DCMS should consider the wider problem of online manipulation and will need to work closely with other departments in their respective policy areas, commissioning expert advice from them when necessary. In designating this responsibility, I hope this will facilitate a unified areas approach that aligns a range of cross-government activity."*

37. Reflecting the direction from Downing Street, DCMS ensured that the CDC was a cross-government team led by DCMS and comprised the departments referred to at paragraph 32 above. The CDC was not envisaged to be a permanent team and would only be operational during a period of heightened risk, such as an election, where there was an increased likelihood of significant disinformation being disseminated with the aim of causing harm to the UK. The CDC was the first formal structure designed to operationally manage disinformation impacting the UK. The structure was trialled during the European Parliamentary elections in April 2019 and was stood up for the 2019 General Election, which took place on 12 December 2019.

38. In addition to considering disinformation which posed risks to the integrity of elections, DCMS also considered concerns raised around public health disinformation. During

the first half of 2019, at the request of DHSC and in response to their concerns about the link between mis and disinformation online and a broad decline in vaccination uptake, working-level discussions were held with DCMS policy officials to discuss DCMS's approach to mis and disinformation.

39. Following this engagement, DHSC and DCMS began a dialogue around the inclusion of disinformation in the White Paper, and how anti-vaccine content fitted within that regulatory framework. DHSC was subsequently invited in the first half of 2019 to join the cross-government counter disinformation working group. This was an informal group created to forge links between relevant departments and to build a wider counter disinformation community.

Regulation

40. Prior to the pandemic there was no single piece of legislation which protected the public while online. Instead, there was a series of legislative and regulatory measures in place which related to specific types of online activity and the potential harms that those activities could generate. However, this meant that the regulatory environment was fragmented and there were gaps where no legal protections were in place.

41. The White Paper, at pages 33-34 **[EM8/06 - INQ000610032]**, provided a high-level summary of the regulatory framework that was in place at the time in relation to online safety which included:

a) GDPR and the Data Protection Act which was enforced by the ICO. This included the collection and use of personal data, including when online. The GDPR had extraterritorial scope and could be enforced against companies outside the UK who offer services to UK users.

b) The Electoral Commission which 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 is also enforced by the police, who lead on the Representation of the People Act offences. The Electoral Commission has powers to investigate breaches of the rules to funding and spending for election and referendum campaigns, which includes digital campaigning.

c) Forthcoming age verification requirements for online pornography. The Digital Economy Act 2017 provided for the regulation of providers of online commercial pornography to ensure that pornographic material is not normally accessible by those under 18, and that content which is deemed to be extreme pornographic material is not made available to any user (those provisions were never commenced).

d) The Equality and Human Rights Commission had oversight of the Equality Act 2010 and the right to freedom of expression, as protected under the European Convention on Human Rights and the Human Rights Act 1998, which would apply to online activity.

e) Ofcom had oversight of video-on-demand services. The EU's Audiovisual Media Services Directive 2010 provided Ofcom with the power to regulate editorial content (programming) on UK 'video-on-demand' services – overseeing compliance on content requirements that cover protecting under 18s, preventing incitement to hate, and commercial references in programmes.

f) The revised EU Audiovisual Media Services Directive 2018, which was to introduce new high-level requirements for video sharing platforms such as YouTube. The revised directive was to place 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 incites violence and/or hatred, and introduce basic requirements around advertising. At that point, a regulator was in the process of being selected, and deadline for implementation was September 2020.

g) The Gambling Commission had responsibility for the licensing and regulation of online gambling. DCMS had worked with the Commission to tighten advertising rules on gambling and launched GAMSTOP, the online self-exclusion scheme.

Additional age verification requirements were expected to take effect in from May that year.

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

General

42. Both the Green Paper **[EM8/05 - INQ000598414]** and the White Paper **[EM8/06 - INQ000610032]** outlined the range of support which was available to children and parents prior to the pandemic about online harms, including misinformation and disinformation and staying safe online. The majority of initiatives were led by civil society groups, regulators, or tech providers themselves. There were some government-funded initiatives, such as the Diana Award Anti-Bullying Campaign, which trained young people to be Anti-Bullying Ambassadors, promoting online and offline safety to their peers. The government also funded the UK Safer Internet Centre to develop cyberbullying guidance which provided advice for schools on understanding, preventing, and responding to cyberbullying, and an online safety toolkit to help schools deliver sessions through PSHE about cyberbullying, peer pressure and sexting.

43. Given the existing range of resources for children and parents, but recognising that there were also '*notable gaps in provision and that adults need support too – for themselves but also as parents*', the White Paper set out government's intention to take a convening role by undertaking to conduct '*a comprehensive mapping exercise to identify what actions are already underway, and to determine the objectives of an online media literacy strategy*' **[EM8/06 – INQ000610032]**. The draft objectives included ensuring: that users were more resilient in dealing with mis and disinformation, including in relation to democratic processes and representation; that people were equipped to recognise and deal with a range of deceptive and malicious behaviours online, including catfishing, grooming and extremism; measures were taken to prevent people with disabilities being excluded from digital literacy education and support, and; the development of media literacy approaches to tackling violence against women and girls online.

44. Media literacy is a tool which can help tackle a wide variety of online safety issues for all internet users, including children. Media literacy means that online users:

    a) have an understanding that online actions have real-world consequences,

    b) have the ability to critically evaluate online information, and

    c) can contribute to a respectful online environment.

45. Evidence shows that improving internet users' media literacy skills builds resilience to dis and misinformation. Media literacy also encourages users to engage in positive interactions and to stand against harmful online behaviours, including online harassment and misogyny. Prior to the Act, which updated and provided greater specificity to Ofcom's media literacy duties in relation to regulated, the Communications Act 2003 required Ofcom to promote media literacy in relation to electronic media generally.

46. As set out in the Green Paper, DCMS and DfE aimed to ensure compulsory school subjects in England addressed challenges experienced by young people online, with both departments responsible for generating the 'online safety' aspects of these subjects. Both planned to conduct thorough and wide-ranging engagement and consultation as part of this. The DfE was in the process of making Relationships Education compulsory for all primary pupils, Relationships and Sex Education compulsory for all secondary pupils, and Health Education compulsory for all pupils in all primary and secondary state-funded schools in England. I understand that DfE consulted on draft guidance for these subjects, which included proposed guidance on how to stay safe online, how to critically consider online information, how people present themselves online and the benefits of rationing time spent online.

47. In the Green Paper, DCMS committed to working with DfE to ensure that children's critical thinking skills would be enhanced through digital literacy to help them recognise "fake news" and intentionally misleading information on the internet.

Pre-pandemic planning

48. The Security and Online Harms Directorate did not conduct pre-pandemic planning in relation to the online safety of children and young people. It was not therefore involved in any pre-pandemic planning relating to the provision of remote education in the event of a national emergency, or more generally. These issues relate directly to the provision of education, which sits within the remit of DfE, who would therefore be better placed to assist the Inquiry in this regard.

Section D - Pandemic picture (knowledge) 1 January 2020 to 28 June 2022 (the "Specified Period")

Work to understand patterns of online behaviour

49. During the pandemic DCMS did not conduct any of its own research to assess the impact the pandemic was having on children's online lives. However, work continued to analyse responses to the White Paper consultation, to develop a regulatory framework and prepare a draft bill which would establish an online safety regulatory framework **[EM8/19 - INQ000606810]**, as well as producing and publishing guidance detailed below at paragraph 62.

50. On 12 February 2020, the government published an initial response to the White Paper consultation **[EM8/20 - INQ000552520]** which provided an overview of the responses to the consultation and wider engagement with stakeholders on the White Paper's proposals. This initial response provided thematic summaries of the responses to each of the consultation's 18 questions and an overview of the feedback in response to engagement with stakeholders. While this response did not provide a detailed update on all the policy proposals, it did give an indication of the government's direction of travel in a number of key areas which had been raised as overarching concerns across some of the responses, such as freedom of expression, the types of businesses likely to be in scope and transparency.

51. Subsequently, on 15 December 2020, the government published a full response to the White Paper consultation, which acknowledged that the Covid-19 pandemic had shone a spotlight on the risks posed by harmful activity and content online **[EM8/21 - INQ000598426].** For example, the response acknowledged that the pandemic

'*underlined a much more grave problem; the risks posed to children online*' and cited a report from the Internet Watch Foundation, published in May 2020, which said that '*in a month-long period during lockdown, the Internet Watch Foundation and its partners blocked at least 8.8 million attempts by UK internet users to access videos and images of children suffering sexual abuse*' **[EM8/22 - INQ000610035]**. Furthermore, there was evidence that children were exposed to large amounts of harmful material during lockdown, with a May 2020 British Board of Film Classification report finding that nearly half of children and teens were exposed to harmful online content while in lockdown **[EM8/23 - INQ000610031]**.

52. In addition, the White Paper consultation response noted that the pandemic '*drove a spike in disinformation and misinformation, and some people took advantage of the uncertainty to incite fear and cause confusion*.' The response **[EM8/21 - INQ000598426]** cited Ofcom data suggesting that in week one of lockdown, nearly 50 per cent of people reported seeing information they thought to be false or misleading about the pandemic, with this figure at almost 60 per cent for 18-34 year old respondents.

53. The department continued to use Ofcom's research and reports into social media use to inform online safety policy, although given many of these reports were annual, they did not provide real-time data on children's engagement with online services. Ofcom's annual '*Children and parents: media use and attitudes*' reports do not report children's total time spent online beyond the 2018 Report. However, the 2020/21 report stated that *'Parents found it harder to control their child's screen time during the Covid-19 pandemic and up to half of parents of children aged 5-15 said they had to relax some rules about what their child did online during 2020'* **[EM8/24 - INQ000560772]**. The 2020/2021 report findings included the below, although some of these statistics will partially cover time spent on activities not covered by the OSA regulatory framework, such as certain forms of apps or games which do not fall within scope of the OSA:

a) gaming seemed to be increasing in popularity among girls - 'video games' moved up to third place in the list of favourite hobbies among girls, from seventh place in 2019 (while being in the top two for boys, both years). Children aged 12-15 reported the longest time playing at 1 hour 28 minutes per day – an increase of nine minutes since 2019. The main driver for the overall increase among 5-15 year olds was

among younger boys aged 5-7 years old. Boys in this age group showed an increase of 24 minutes since 2019, to 1 hour 26 minutes in 2020.

b) in 2020, almost half of 8-11 year olds and almost six in ten 12-15 year olds said they had used sites or apps that they had not used before. Within this group, one in ten in each age group said they had tried 'lots' of new sites and apps during the year. The younger age group in particular were more likely than in 2019 to use newly discovered sites or apps – which could be due to online home learning, or to finding alternative forms of entertainment online.

54. It can be difficult to establish a causal relationship between time spent online and/or online activities participated in by children and their life outcomes. However, some relevant findings from the Ofcom 2020/2021 report included:

a) just over half (55 per cent) of 12-15 year olds had had some form of negative online experience.

b) among these negative experiences, the most likely to be cited was "being contacted by a stranger online who wanted to be their friend" (30 per cent). However, three-quarters of 12-15 year olds knew how to block messages on social media from someone they did not want to hear from; more than half had done this (55 per cent).

c) about a fifth of 12-15 year olds said they had accidentally spent money online that they did not mean to, seen or received something scary/troubling, or seen something of a sexual nature that made them feel uncomfortable.

d) overall, half of 12-15 year olds said they had encountered hateful content online in the past year, with eight per cent saying that they had seen it often. Hateful content was defined as being anything that had been directed at a particular group of people based on their gender, religion, disability, sexuality, or gender identity.

55. To improve knowledge of the available evidence on the risks and impacts to children from harmful content and activity on services within the scope of the Bill, following a tender process which commenced in September 2021, DCMS commissioned the

National Centre for Social Research and City, University of London, to carry out a rapid evidence assessment (**"the REA"**), which was subsequently published on 27 May 2022 **[EM8/25 - INQ000609980]**. DCMS commissioned this research in order to improve its evidence base on what it regarded as key harmful online behaviours. This was to inform the development of its policies on primary priority content and priority content, which is harmful to children, which would subsequently become part of the Bill. The REA included a synthesis of evidence on the definition, prevalence and impacts of harmful content and activity, as well as any variation amongst different groups of children, including children of different age groups, genders, ethnicities, religions, sexual orientations, and social backgrounds. The REA focused on harmful content and activity, the scope of which was guided by the harms listed in the White Paper, which included cyberbullying, pornography, violent content, pro-self-harm content, pro-suicide content, and content which could give rise to eating disorders. It also looked at emerging or lesser researched harmful content and activity. The REA included a summary of the evidence available on:

a) the impact of cyberbullying on the wellbeing, mental health, education and social relations of children and young people targeted by this behaviour.

b) impacts on wellbeing, mental health, attitudes and behaviour towards sex and relationships and attitudes towards women and girls from viewing pornography.

c) the impacts of accessing self-harm and suicide online content, including exacerbating self-harming behaviour, potentially exacerbating suicidal ideation, and evoking negative emotions.

d) the impacts of viewing pro-eating disorder content.

56. The REA found that a large amount of research on online harms was outside its scope. Reasons for this included the prevalence of international studies which lacked UK-specific data and the ethical challenges in researching children's online activities. Topics like cyberbullying and pornography had been researched extensively, but that research had inconsistent findings, while limited exploratory research had been conducted on areas such as self-harm and eating disorders. Emerging harms, including alcohol consumption, dangerous stunts, and misinformation, were the subject of minimal research due to their evolving nature. The evidence base also faced

methodological issues such as inconsistent definitions, differing measurements of prevalence and impact, variable age definitions and a generalisation of online platforms.

57. DCMS's priority during this period was initially to focus on getting the Bill ready to be introduced in parliament. This work included developing and refining online safety policies for inclusion in the Bill, working with parliamentary counsel to ensure that the Bill clauses met the policy objectives and stakeholder engagement. DCMS' focus then shifted to the parliamentary passage of the Bill. This work was vital to make online services which were in scope of the Bill safer, particularly for children, as detailed in further below. Therefore, DCMS did not conduct work to specifically assess the extent to which the pandemic had a longer-term impact on children's online lives. Although the Bill was DCMS' focus at this time, it did not mean that DCMS did not undertake work to protect children from online harms during the pandemic and details of this additional work are referred to at paragraph 62 below.

Online safety and harm

58. As detailed above, the department drew on a range of research and assessments to develop an understanding of the risk of online harm to children and young people, including how those risks changed during the pandemic.

59. The department's primary response to online safety was via the Bill and DCMS was therefore focused on developing the various clauses of the Bill and ensuring its passage through parliament. Additionally, DCMS worked on an impact assessment for the Bill, which was published on 27 January 2021 **[EM8/26 - INQ000610028]**. The Bill went through pre-legislative scrutiny by a joint committee which published its report in December 2021 **[EM8/27 - INQ000610027]**. The report specifically highlighted the risk of harm to children and considered the Bill's relevant protections. The Bill was subsequently introduced in the House of Commons in March 2022, and was subject to scrutiny from both Houses.

60. HO is the lead department for tackling child sexual abuse online and shared responsibility for the publication of the White Paper and subsequent government

responses to its consultation, all of which included details of the government's planned response to online CSEA. Additionally, HO led the Interim Code of Practice on Online CSEA, which was co-published by DCMS on 15 December 2020 **[EM8/28 - INQ000610036]**. Later HO published the Tackling Child Sexual Abuse Strategy in 2021 **[EM8/29 - INQ000552859]**.

61. Therefore, although DCMS was aware during the pandemic of evidence relating to online CSEA, which then informed its online safety policy, HO as lead department for CSEA held overall policy responsibility for government's efforts to tackle it. As such, DCMS did not monitor any trends or increases in availability of or access to online child sexual abuse or CSEA material, including indecent imagery and other harmful material.

62. In addition to the Online Safety Act, DCMS delivered a range of work during the pandemic to support children and young people in relation to their internet use. For example, in April 2020, DCMS published guidance on Covid-19 online safety on Gov.uk, which focused on how to keep children and young people safe online and build their ability to spot harmful false narratives online **[EM8/30 - INQ000598450]**. The Minister for Digital and Culture at that time, Caroline Dinenage, hosted a roundtable with children's charities to coincide with the launch of the guidance **[EM8/31 - INQ000361199, EM8/32 - INQ000361207].** This was followed in October 2020 by DCMS's announcement of the launch of a new internet game, 'Go Viral', developed between DCMS, CO and the University of Cambridge, aimed at helping young people build their resilience to the spread of mis and disinformation online. The game aimed to demystify how disinformation was produced, giving players an idea of the techniques and motivations behind the spread of Covid-19 related disinformation, and pre-emptively exposing people to the methods which malign actors used to disseminate online falsehoods. Within the first month of its release the game had been played approximately 33,000 times since its launch, which exceeded DCMS' expectations.

63. In December 2020, the UK Council for Internet Safety (**"the UKCIS"**) and DCMS published advice for education settings working with children and young people on how to respond to an incident of nude and semi-nude images being shared, replacing guidance which had been given in 2016 **[EM8/33 - INQ000610037]**. The UKCIS is a collaborative forum - established by the government - through which academics,

technology companies and the third sector work together to ensure online safety for the UK. UKCIS meetings had previously been chaired by ministers from DfE, the HO, and DCMS (prior to responsibility for UKCIS transferring from DCMS to DSIT). DCMS's role in the development of this guidance was to provide some of the secretariat functions to arrange UKCIS meetings. UKCIS members led on the drafting of the guidance, which was shared with DCMS prior to publication.

64. Additionally, during the pandemic DCMS conducted regular engagement at all levels with social media platforms to discuss online safety trends. Sometimes this engagement with platforms was through the CDC's regular meetings with platforms (see paragraph [94] onwards), during which meetings other online safety issues would infrequently be added to the agenda for discussion. Industry feedback from engagement with Facebook, TikTok and X (formerly known as Twitter) suggested that their focus remained on tackling illegal content, particularly CSEA material. Industry feedback also indicated an increased use of these services as a result of Covid-19 lockdown measures and a corresponding increase in user-reporting of harmful material/behaviour.

65. In April 2021 the UK, Canada, France, Germany, Italy, Japan, the US, and European Union agreed to the G7 Digital and Technology Ministerial Declaration, under the chairmanship of the DCMS Secretary of State **[EM8/34 - INQ000610026]**. This declaration included the agreement of internet safety principles for G7 countries. The UK held the G7 presidency in 2021 and DCMS led on the development and negotiation of these principles.

66. In June 2021, DCMS published guidance on the principles of safer online platform design which gave guidance to those designing an online platform on how to reduce the risk of harm for those who use it, including examples of good practice **[EM8/35 - INQ000610038]**.

Misinformation/disinformation

67. During the pandemic there was a large increase in the amount of online mis and disinformation on a number of topics, including links between 5G masts and the virus, vaccines, and bogus cures. DCMS therefore stood up the CDC, as will be set out in

further detail below, to understand the prevalence of mis and disinformation and work with social media platforms to promote authoritative sources of information.

Legal Framework

68. The CDC, and subsequently the CDU, took active steps to operate in compliance with all applicable legislation including, but not limited to:

a) the Human Rights Act 1998, which incorporates the rights contained in the European Convention on Human Rights.

b) data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA); as well as

c) ensuring its work did not amount to surveillance as described in the Regulation of Investigatory Powers Act 2000 (RIPA).

69. In order to comply with the team's legal obligations, staff were aware of the applicable legislation and the consequences of failure to comply with any applicable legislation i.e. enforcement or other action, such as legal proceedings, being taken against DCMS. Additionally, the CDC and later the CDU had a series of processes and checks in place to ensure that legislation was complied with. For example, staff had to be satisfied that all data monitoring and analysis which they conducted was lawful, necessary, and proportionate, and that they had the appropriate internal legal advice and senior approvals. This approach was later codified in the CDU's compliance policy **[EM8/36 - INQ000361185]**. As part of its evolution into a permanent team, the CDU began the process of codifying the existing processes and policy into a single compliance policy in Autumn 2021, collaborating with both external legal advisors and Government Legal Department. This policy was iterated over 2022, and the wording was finalised in March 2023 and circulated to all CDU staff on 4 April 2023. It was regularly reviewed and amended where needed and all new joiners were required to familiarise themselves with the content as part of their induction.

70. To understand the trends and activity in the agreed areas referred to in paragraph 78 below , the CDC/CDU, or its external contractor, carried out searches of open, online

public spaces, predominantly across the major social media platforms, using key words and terms which were related to the three areas of focus referred to in paragraph 78 and then further refined based on the most relevant risks at the time. Where the CDC/CDU used in-house tools to conduct searches, the key words and terms used determined which data sources would be identified and reviewed, i.e. search results would only contain social media posts which contained those key words and terms. In order to remain within the scope agreed by ministers and its legal obligations, the CDC/CDU only used open-source information i.e. information which was freely available and in the public domain. This focused approach meant that the CDC/CDU did not seek out, nor aim to respond to, all incidents of mis and disinformation. Its sole focus was on trends and narratives which appeared online, and it did not therefore conduct searches of individuals.

71. When the CDC/CDU monitored mis and disinformation trends and narratives, sometimes personal data belonging to an individual, such as a social media user handle, was collected as a by-product of fulfilling its role. Where such data was collected, the CDC/CDU anonymised it wherever possible. However, there were circumstances where it was not possible to anonymise all personal data. For example, where a piece of content was harmful and in breach of a platform's terms of service, it was necessary to retain a link to the post, (which could contain personal data such as the author's name or social media handle), to facilitate a referral to the social media platform on which that content had been posted. Another example would be where the post contained disinformation about a third party, which was harmful and in breach of a platform's terms of service. In this circumstance the third party's details would be retained, again so that the content could be referred to the relevant platform if necessary.

72. The CDU published a privacy notice on Gov.uk which set out the legal basis on which the CDU handled any such personal data to comply with UK GDPR and DPA 2018 **[EM8/37 - INQ000474309]**. The CDU's policy was to keep such personal information for no longer than was necessary and in any event for no longer than two years. However, due to the need to preserve evidence for the Inquiry, it has been necessary to retain some personal data which would have normally been deleted. This will be retained until the Covid-19 Records Preservation and Retention Order has been lifted.

It is anticipated that the Covid-19 Inquiry will continue until 2026 and therefore it is expected that the Order will not be lifted before then.

73. Both the CDC and the CDU were committed to protecting freedom of expression in line with the UK's democratic values and did not seek to limit or impact political debate or opinion. This was not, and never had been, its role. The CDC and CDU continually developed and implemented solutions to the challenges of mis and disinformation which were consistent with our principles and values: protecting freedom of expression and promoting a free, open, and secure internet.

74. The CDU compliance policy contained specific measures which dealt with the issue of freedom of expression. For example, the policy stated that the CDU respected freedom of expression and did not seek to capture genuine political debate. For this reason, in accordance with the policy, neither the CDC or the CDU escalated any online content to social media platforms which came from a parliamentarian or other elected official (of any party), journalist or established news outlet.

75. In order to ensure this right was protected, staff working in the CDC/CDU were provided with escalations guidance and principles **[EM8/37 - INQ000474309]**. These set out how to identify whether information was false or misleading and how to assess whether it was capable of causing harm. In addition, the guidance set out what staff should consider when looking at any potential impact on freedom of expression. In particular, it recognised the need to balance the right to freedom of expression against the potential harm which the information could cause. To ensure that these principles were being applied correctly and to ensure that content was not referred to platforms erroneously, a second, more experienced or more senior, member of the team would review every recommendation to refer content to platforms. That member of staff would ensure that the escalations guidelines had been applied correctly and that it was appropriate for the content to be referred. Where a case was complex, for example where the question of whether a platform's terms of service had been violated was not straightforward or considered to be a borderline one, that decision would be reviewed by someone at SCS level.

Operational Response

76. On 5 March 2020 DCMS stood up the CDC in response to the acute mis and disinformation risks emerging from the Covid-19 pandemic. The CDC drew on a range of cross-government teams, bringing together relevant expertise from CO, HO and FCDO. Where the CDC's work on disinformation included examples which could potentially be state sponsored disinformation, it also engaged with the UK Intelligence Community, where required. At its peak, the CDC as a whole, including staff from the other key departments referred to above, was formed of up to 50 staff. However, this figure is an estimate as the CDC was flexible in nature, with DCMS and other departments pulling on their wider resources (which may not have been solely focused on mis and disinformation) as needed in order to reach common objectives. DCMS can only be certain in its figures for its own staff. In DCMS, core staffing levels within the CDC varied between 6-10 full time equivalents (**"FTE"**). Additional staff (surge capacity) were brought in wherever needed, including for the pandemic response, when the DCMS staff in the CDC reached around 25 FTE at its peak. During the busiest period for the CDC (April to June 2020), it was operational seven days a week, with extended operating hours, resulting in DCMS core and surge staff working in a shift pattern.

77. The CDC was the principal way in which DCMS approached the threat of mis and disinformation during the pandemic and its remit was focused on risks to public health, public order or safety, the targeting of minority or vulnerable groups and disinformation targeting the UK's national security. Although the CDC did not have a specific remit in relation to mis and disinformation aimed at children and young people, they would have still been included within this remit. The CDC's role included work in the following key areas:

a) the analysis of potentially harmful online trends and narratives (involving mis and/or disinformation) where they present a risk to public health, public safety, or national security and collaborating closely with analytical teams across government and external monitoring partners.

b) the sharing of insights into the range of false and misleading narratives identified with other relevant teams across government, including teams in DHSC who led on vaccine related communications campaigns **[EM8/38 - INQ000361168]**.

c) engagement with social media platforms on the promotion of mis and disinformation relating to Covid-19 vaccines in line with platform terms and conditions and the promotion of authoritative sources of information. The CDC was given 'trusted flagger' status by X (formerly known as Twitter), YouTube, Meta, and TikTok to enable the CDC to swiftly flag content to platforms which was deemed likely to violate their terms of service.

78. Departmental ministers reviewed the position and decided the areas on which the CDC should focus its efforts. Those areas were ones where there was content, or the potential for content, targeted at UK audiences which posed a risk of harm to public health, public safety, or national security. The CDC did not have a specific remit in relation to children and young people, however mis and disinformation which was targeted at them and fell within one of these risk categories would have fallen within the CDC's remit.

79. Where harm fell outside these three specific categories, that harm fell outside the CDC's remit and did not form part of its monitoring work. For example, harm to the government's political agenda would not have been part of the CDC's remit. There may have been circumstances where there would be some overlap between the three areas of focus above and areas of political interest. In those instances, the CDC focused solely on potentially harmful mis and disinformation narratives which fell within those three specific areas; its focus was not on social media posts or commentary which was critical of government policy. The civil servants working within the CDC were also bound by the Civil Service Code, which requires civil servants to be politically neutral.

80. As set out in more detail below, the CDC worked with external partners during the pandemic in order to enhance and increase its understanding of mis and disinformation online. This work focused primarily on the mainstream platforms mentioned above and complemented the open-source monitoring conducted by other analytical teams (such as those in the CO, HO, FCDO, and UK Covid Vaccine Security (UKCVS)). In addition to mainstream platforms, misleading narratives about vaccines also emerged from smaller, fringe platforms, blogs and financially motivated "junk news" websites **[EM8/39 - INQ000361196]**.

81. A large amount of the mis and disinformation encountered by the CDC related to Covid-19 vaccines and a number of key narrative themes were identified by the CDC such as:

    a) medical misinformation around vaccines which could undermine vaccine confidence, e.g. claims that vaccines genetically modify human DNA or contain harmful, mercury-based chemicals.

    b) online narratives falsely connecting Covid-19 and vaccines to 5G technology which could lead to physical violence or abuse.

    c) conspiratorial claims which incorporated vaccine mis and disinformation into pre-existing narratives, e.g. claims that Covid-19 vaccines contained "nanobots" and were intended as a deliberate form of population control.

    d) mis and disinformation targeting minority or vulnerable groups, such as claims that a particular ethnic group would be used as "guinea pigs" to test the vaccine Some of these themes were set out in a paper in September 2020 **[EM8/38 - INQ000361168]**.

82. Over the course of the pandemic response during 2020, the government moved away from having a temporary structure which was comprised of staff from various departments and the CDC evolved into the CDU, a permanent DCMS (subsequently DSIT) team. This did not mean that cross-government cooperation ceased: the CDU continued to work closely with colleagues from across government on a number of issues, as well as sharing its insights on the information environment.

83. The CDU was different in makeup and intent from the CDC: the latter was a temporary virtual cross-government structure of which the DCMS disinformation team was a part, whereas the CDU was a permanent team based within a single department which collaborated with other departments as needed and determined by the content in question. As the government wound down its work on Covid-19, so too did the CDC and it transitioned to the smaller, permanent CDU. This coincided with the gradual

ramp up of government focus on Russian activity in early 2022, in the build up to its invasion of Ukraine, and then the significant increase in work to respond to the invasion and the information threats that this posed.

Use of External Suppliers

84. In April 2020, the CDC began to use external suppliers to assist with the monitoring of mis and disinformation, as a direct consequence of the pandemic. DCMS signed contracts with three external monitoring suppliers as part of the CDC's response to the Covid-19 pandemic. Two of these suppliers, Global Disinformation Index and Digitalis, were selected through direct awards due to reasons of extreme urgency. The direct award process was conducted in line with Procurement Policy Note 01/20: Responding to Covid-19 **[EM8/40 - INQ000361205]**.

85. The contract with Global Disinformation Index ran from 23 April 2020 to 22 October 2020. The aim was to assist the CDC to identify disinformation narratives related to Covid-19 and understand how these were spreading on platforms which the CDC did not have any engagement with. DCMS did not extend or renew this contract upon its expiry. The contract with Digitalis was a short-term contract which ran from 4 May to 3 June 2020. The aim of this contract was to provide the CDC with insights on online search terms related to Covid-19. This was so the CDC could understand the extent to which UK audiences were being exposed to mis and disinformation. Again, DCMS did not extend or renew this contract upon its expiry.

86. In December 2020, the CDC ran an accelerated open procurement exercise. The purpose of the exercise was to identify an external supplier who could enhance the CDC's understanding of mis and disinformation which posed a risk to UK audiences, by monitoring and analysing Covid-19 mis and disinformation online. The Logically Ltd (Logically) was chosen to provide this service via the procurement exercise. The parties entered into a contract for the period 1 January to 31 March 2021. This was extended twice, in line with the agreed contractual terms, to cover the period 1 April to 30 June 2021 and 1 July to 31 August 2021, while a further tendering process was underway.

87. Logically was successful in two subsequent open procurement exercises. One was for the period 1 September 2021 to 30 June 2022 and the other was a contract covering the period 1 July 2022 to 31 March 2023, which was subsequently extended until 31 August 2023. This contract was not renewed or extended when it ended, with the CDU opting to use a different supplier.

88. During those contracts Logically used proprietary open-source tools and AI technology to provide monitoring of online mis and disinformation narratives. Both DCMS and Logically were required to adhere to the policies and procedures set out in the CDU's compliance policy and had to take all steps to minimise the collection of any personal data and anonymise where possible any unavoidably collected personal data. Furthermore, the contractual obligations prevented Logically from monitoring individuals. The monitoring from Logically provided CDC/CDU analysts with insights needed to identify and assess harmful content online.

89. The CDC's role was to understand the information environment as a whole. Consequently, the team and its external contractors focused on the mis and disinformation itself, rather than the identity of the poster or any particular groups at which it was aimed. This meant that neither the CDC nor its external contractors focused their work on mis and disinformation which was specifically targeted at children. It is not therefore possible to provide specific examples of content or types of content which was specifically targeted at children or content with which children engaged. However, it is almost certain that some of the content which was identified by the CDC and its external contractors would have been viewed by children. The CDC did not specifically look at the impacts which pieces of mis or disinformation had on the individuals who had viewed them. Consequently, it is not possible to assess what impact specific pieces of content viewed by children would have had.

The Counter Disinformation Policy Forum

90. On 3 November 2020, the DCMS Secretary of State hosted a joint roundtable with the DHSC Secretary of State **[EM8/41 - INQ000361169] [EM8/42 - INQ000361189]** and invited major social media platforms, civil society, and health experts to address the specific issue of harmful and misleading narratives, particularly around Covid-19 vaccines. Social media companies agreed to continue to work with public health bodies

to ensure that authoritative messages about vaccine safety reached as many people as possible, to commit to swifter responses to flagged content and to commit to the principle that no user or company should directly profit from Covid-19 vaccine mis and disinformation.

91. At the agreement of the joint roundtable, DCMS established the Counter-Disinformation Policy Forum. This brought together representatives from the social media companies, academics, fact-checkers, and researchers with the aim of improving understanding of the information environment, developing, and improving the responses to mis and disinformation and further exploring future approaches and policy recommendations. A copy of the forum's terms of reference are attached at **[EM8/43 - INQ000361181]**.

92. The Counter-Disinformation Policy Forum met five times between 2 December 2020 to 10 June 2021 to discuss shared approaches to countering Covid-19 mis and disinformation, with a particular focus on anti-vaccination narratives. The forum was focused on the information environment as a whole, rather than on specific issues which affected children and young people. However, the issues which the forum focused on would have included those which children and young people encountered online during the pandemic e.g. vaccine mis and disinformation.

93. In the context of the pandemic, the Counter-Disinformation Policy Forum demonstrated the value of a whole of society approach to mis and disinformation, facilitating the sharing of trends and research updates relating to Covid-19 and vaccines between platforms, civil society, academia, and government. Stakeholder engagement following the conclusion of the forum demonstrated that the early sharing of research was more efficient, inspired follow up research and helped inform longer term understanding of disinformation ecosystems and response effects. Several academics reshaped aspects of their current projects based on presentations from other members.

Engagement with Social Media Companies

94. The CDC worked with social media platforms (predominantly Meta (formerly known as Facebook), X (formerly known as Twitter), Google, YouTube and TikTok) to

understand their terms of service, encourage the consistent application of those terms of service and to share insights into how narratives and trends were developing in the information space. Sometimes the CDC also acted as the liaison between other government departments and social media platforms to encourage authoritative sources to be actively promoted on their sites.

95. Where developments in technology or harmful behaviours from particular groups (e.g. malign states or state-linked activity) emerged that platforms' terms of service were not immediately designed to counter, the CDC/CDU worked with platforms to encourage these to be developed and/or for other measures, such as promoting authentic content, to be deployed. The strong relationships developed with the major social media platforms during the pandemic enabled the CDC/CDU to respond more quickly and effectively to acute disinformation risks both during the pandemic and subsequently.

96. An example of how this worked in practice was in early 2020 when disinformation narratives linking 5G and Covid-19 were amplified widely online. This resulted in real-world damage to mobile phone cell towers. The CDC worked closely with social media platforms to ensure their policies regarding this content were updated in light of this narrative. A dedicated Gov.uk page was created, linking to the World Health Organization (WHO) and a fact-checking organisation's content on the narrative **[EM8/44 - INQ000361200]**. A link to this page was then served up by X (formerly known as Twitter) under a 'know the facts' header when users searched for 5G and covid/coronavirus within the platform. This represented a significant piece of work for the CDC, working with the DCMS communications team, which had been commissioned and closely monitored by ministers, who were concerned that damage to the telecommunications network could cause harm to the public, e.g. people being unable to contact the emergency services.

97. If content was identified which had the potential to cause harm under one of the categories highlighted in paragraph 78 and appeared to violate a platform's terms of service, the CDC/CDU could notify the relevant platform. The CDC/CDU had what is known as `trusted flagger' status with the major platforms. A 'trusted flagger' could be an individual or entity, including civil society groups or academics, who were considered by a service provider to have particular expertise in or responsibility for

tackling harmful online content. Trusted flagger status meant that the CDC/CDU was swiftly able to highlight any potentially harmful content, and that the referral was prioritised by those platforms.

98. Although the CDC/CDU had trusted flagger status, it was then up to the platform to decide whether or not to take action against the content which the CDC/CDU had highlighted, based on the platform's own assessment of the content against their terms of service. The CDC/CDU did not have the power to force the platform to remove that, or indeed any, content, nor did it have any influence over its decision.

99. Following the engagement which the CDC/CDU had with social media platforms, many of them implemented policies and procedures to counter the spread of harmful and misleading narratives related to Covid-19 vaccines. These included:

a) Meta (formerly known as Facebook) announcing in December 2020 that they would remove content featuring harmful, false, or misleading narratives about Covid-19 vaccinations where it had been debunked by health experts, as well as directing users to authoritative sources such as the NHS website. Meta also displayed warnings on Facebook on more than 190 million pieces of Covid-19 related content that its fact-checking partners rated as false, partly false, altered, or missing context. In September 2021, Meta reported that it had removed more than 20 million pieces of false Covid-19 and vaccine content.

b) X (formerly known as Twitter) announcing in December 2020 that they would remove tweets making false or misleading claims about Covid-19 vaccinations. In December 2021, X reported that it had removed over 65,000 pieces of content and suspended over 3,000 accounts globally for violations of its Covid19 guidance.

c) YouTube introducing information panels on its videos containing links to accurate information about Covid-19, including from the NHS, and banning content that contradicted expert consensus from health authorities such as the NHS or WHO. In September 2021, YouTube reported that it had removed over 130,000 videos for violating its Covid 19 vaccine policies.

d) TikTok prohibiting content which was inaccurate or false and which caused harm to individuals, the platform's community, or the larger public. From April to June 2021, TikTok removed 26,000 videos for Covid-19 mis and disinformation. TikTok also introduced a Covid-19 Information Hub where its users could find answers to questions about the virus and vaccines from authoritative sources which was viewed 921 million times globally between April and June 2021.

100. As mentioned at paragraph 97 above where the CDC/CDU identified content which violated a platform's terms of service, this could be flagged to the relevant platform who then decided on the appropriate response. This work helped to alert platforms to activity where enforcement of their own policies needed to be improved. Content flagged by the CDC/CDU was vastly outnumbered by the overall volume of content moderated by platforms, as referenced in paragraph 99 above. The wider engagement with platforms that the CDC and CDU undertook during the pandemic was the more significant element of this relationship, ensuring risks from mis and disinformation were mitigated as far as possible.

101. The CDC observed that platforms took a significant number of positive steps to respond to the challenge of mis and disinformation during the pandemic. Their approach evolved over time to adapt to the changing nature of the mis and disinformation content on their platforms. During the pandemic, DCMS (through the work of the CDC/CDU), and other departments across government, engaged with the platforms at both official and ministerial level to encourage platforms to take a number of steps, including to:

a) continue to develop their technological capabilities for detecting and removing disinformation as well as other harmful content.

b) ensure that their users were fully informed of the risks of mis and disinformation on their platforms and the steps they could take to protect themselves; and

c) provide greater transparency on the actions that platforms were taking to tackle this kind of content, including improving access for researchers to better understand the scale, scope and impact of mis and disinformation.

102. Children aged between 12 and 17 were entitled to receive the Covid-19 vaccine from September 2021. Therefore, the work which the CDC did with social media platforms to reduce the amount of mis and disinformation surrounding the vaccine and to promote authoritative content, would have been beneficial to children within that age group. Additionally, the more general work which the CDC did with the major platforms to improve their response to mis and disinformation protected children by reducing their exposure over the course of the pandemic to harmful mis and disinformation.

103. There was no regulatory regime in operation during the pandemic which governed online mis and disinformation on social media platforms. It was an area that required significant collaboration between government and social media platforms, including negotiation with individual platforms about their specific approach to similar circumstances. The Act **[EM8/03 - INQ000642745]** introduced duties on social media platforms to address certain kinds of mis and disinformation online.

Media literacy

104. As far as I am aware, DCMS did not conduct any work on media literacy which specifically considered the impact of, or plan for, children moving to primarily online learning during the pandemic. However, during this period, DCMS did conduct general media literacy activity which had positive implications and benefits for children's online safety.

105. In April 2020, DCMS, in partnership with DfE, published guidance on Covid-19 Online Safety on Gov.uk, which focused on how to keep children and young people safe online and build their ability to spot harmful false narratives online **[EM8/30 - INQ000598450]**.

106. In July 2021, DCMS published the government's Online Media Literacy Strategy [**EM8/45 - INQ000609979]**, which set out the government's plans to improve media literacy across the UK. The strategy outlined key priorities to support all internet users, particularly vulnerable groups, in developing the skills needed to make safer and more informed decisions online.

107. While the strategy did not specifically reference the impact of online learning on children, it recognised the risks to all users caused by sudden increased use of the internet. It also recognised that when users who have not previously used the internet regularly begin to start using it, they are more vulnerable to online harms, due to having lower media literacy levels than those who already use the internet regularly. It was noted that this was of particular concern in the context of the pandemic when many essential services were suddenly only available online.

108. During this period, DCMS delivered various media literacy initiatives as part of the strategy, including initiatives targeted at children. In the financial year 2021 to 2022, £250,000 in grant funding was provided for media literacy organisations to adapt their resources for teachers of children with special educational needs, who were likely to be particularly vulnerable to online harms.

109. The strategy also recognised the importance of platform design in supporting users to make informed and safe choices (i.e. media literacy by design). As mentioned at paragraph 66 above, although not directly in response to the increase in online learning during the pandemic, in June 2021 DCMS published principles of safer online platform design to help businesses and organisations design safer online platforms for their users. This included specific recommendations for supporting children to keep themselves safe when they are online. For example, the principles stated that platforms should *'ensure information like terms of service, or tools used to report harms, are prominent and easy to understand for children of different ages'* and *'set safety, security and privacy settings to high by default'* **[EM8/35 – INQ000610038]**.

Illegal content

110. Responsibility for addressing the immediate risks and impact of illegal content and activity on children during the pandemic, including online CSEA, was a matter for law enforcement. Consequently, this was an area which was led by HO, who will be in a better position to answer the Inquiry's questions on what steps were taken to understand and mitigate these risks.

111. DCMS worked with the HO and the DfE to produce a resource page on gov.uk on child online safety **[EM8/46 - INQ000518754]**. This included advice for parents and carers to keep children safe from a range of harms, including illegal activity such as CSEA, criminal exploitation, violence and gangs, as well as illegal content such as radicalising content and the consensual and non-consensual sharing of nude images/videos ("sexting"), It also included guidance on cyberbullying, age inappropriate content and cross cutting guidance on online safety tools such as parental controls and apps to help children stay safe online.

112. In addition, a second set of guidance was published **[EM8/47 - INQ000518741]** which outlined a number of principles that users should take to stay safe online. This guidance included additional online safety Covid-19 advice for parents, including on the use of parental controls, having effective conversations about online safety with children and staying safe and healthy online by considering controls on screen.

113. As mentioned above, DCMS did not monitor the amount of illegal online content which was produced during the pandemic and did not conduct specific pieces of research to establish whether the volume of illegal content had changed or whether new categories of illegal content had emerged during this period. It is therefore unable to provide an assessment of whether the guidance referred to above was effective in minimising the impact of illegal online content on children. There is external reporting, for example from law enforcement and the Internet Watch Foundation, which suggests that CSEA had increased during the early months of the pandemic. However, as I have previously mentioned, DCMS's priority was to focus on establishing an effective regulatory framework to protect children from harm online, and this included the imposition of duties on providers for tackling illegal content and activity. Subsequently DCMS' priority was to secure the parliamentary passage of the Bill to make in scope online services safer for children.

Primary Priority Content and Priority Content that is harmful to Children

114. As well as protecting children from illegal content and activity, under the Online Safety Act in-scope services that are likely to be accessed by children have a duty to take steps to prevent children from encountering the most harmful legal content, which is designated as 'primary priority' content. This includes pornography and content that

encourages, promotes, or provides instructions for self-harm, eating disorders, or suicide.

115. User-to-user services which are likely to be accessed by children will need to use highly effective age assurance to prevent children from encountering primary priority content where they identify such content on the service. Search services must minimise the risk of children encountering this type of content in or via search results.

116. Services must also put in place age-appropriate measures to protect children from 'priority' content. This includes abusive or hateful content, bullying content, content that encourages or depicts serious violence or injury, or dangerous stunts or challenges and content that encourages ingestion, inhalation, or exposure to harmful substances.

117. DCMS wanted to develop its understanding of the available evidence on the risks and impacts to children from harmful content and activity. It also wanted to understand the prevalence of such content on the different types of online services which were likely to fall within scope of the Bill, DCMS commissioned the REA, referred to at paragraph 55 above **[EM8/25 - INQ000609980]**. The REA included a synthesis of evidence on the definition, prevalence and impacts of harmful content and activity, as well as any variation amongst different groups of children, including children of different age groups, genders, ethnicities, religions, sexual orientations, and social backgrounds. The review focused on harmful content and activity, the scope of which was guided by the harms listed in the White Paper. This included cyberbullying, pornography, violent content, pro-self-harm content, pro-suicide content and content which could give rise to eating disorders. It also focused on emerging or lesser researched harmful content and activity. The paper included a summary of the evidence available on:

a) the impact of cyberbullying on the wellbeing, mental health, education and social relations of children and young people targeted by this behaviour.

b) the impact on wellbeing, mental health, attitudes and behaviour towards sex and relationships and attitudes towards women and girls from viewing pornography.

c) the impact of accessing self-harm and suicide online content, including exacerbating self-harming behaviour, potentially exacerbating suicidal ideation and the evoking negative emotions.

d) the impact of viewing pro-eating disorder content.

e) violent content.

f) online content and activity that promoted stunts and challenges.

g) content and activity that promoted alcohol consumption.

118. The research did not outline any specific increases in the rates of primary priority, priority or non-designated content that may be harmful to children as a result of the pandemic. Overall, as the report outlined there was not a good evidence base on specific harms impacting children: "*there is a lack of primary research that focuses specifically on the prevalence and impacts of content and activity on children and young people in the UK. This is largely due to ethical challenges of conducting research with children and young people across much of the content and activity in scope of this review*" **[EM8/25 - INQ000609980]**.

119. Since 2018, Ofcom's annual Online Experiences Tracker (**"OET"**) **[EM8/48 - INQ000609982]** has surveyed children aged 12-15 years on their exposure to online harms, including categories of harm that align with the primary content set out above. However, the OET changed methodology in 2020 from asking participants about their experiences over the prior 12 months to asking about the prior four weeks. This means that data pre and during pandemic are not comparable and so do not allow tracking over this period.

120. The findings within the REA were used to inform the final list of primary priority and priority harms which were set out in the Bill (now sections 61 and 62 of the Act) **[EM8/03 - INQ000642745].**

a) For primary priority content this is:
   i. pornographic content.
   ii. content which encourages, promotes, or provides instructions for suicide.
   iii. content which encourages, promotes, or provides instructions for an act of deliberate self-injury; and
   iv. content which encourages, promotes, or provides instructions for an eating disorder or behaviours associated with an eating disorder.

b) Content which falls within the definition of priority content is:
   i. content which is abusive, and which targeted any of the following characteristics: race, religion, sex, sexual orientation, disability, or gender reassignment.
   ii. content which incites hatred against people of a particular race, religion, sex, or sexual orientation, who have a disability, or who have the characteristic of gender reassignment.
   iii. content which encourages, promotes, or provides instructions for an act of serious violence against a person, bullying content and content which depicts real or realistic serious violence against a person or depicts the real or realistic serious injury of a person in graphic detail.
   iv. content which depicts real or realistic serious violence against an animal, depicts the real or realistic serious injury of an animal in graphic detail, or realistically depicts serious violence against a fictional creature or the serious injury of a fictional creature in graphic detail.
   v. content which encourages, promotes, or provides instructions for a challenge or stunt highly likely to result in serious injury to the person who does it or to someone else; and
   vi. content which encourages a person to ingest, inject, inhale or in any other way self-administer a physically harmful substance or a substance in such a quantity as to be physically harmful.

121. Overall, the Department's focus was on establishing an effective regulatory framework to protect children online, by developing robust duties on service providers

which could be included in the Bill. A key part of this work was the creation of a specific set of primary priority and priority harms to focus providers' efforts to protect children on their services, as outlined above. These definitions and the decision as to the types of content which fell within them was developed during the course of the pandemic. As previously explained, DCMS' priority at this time was to produce the Bill and ensure its successful passage through parliament.

Non-designated content that is harmful to children

122. As mentioned above, the findings of the REA helped to inform the categories of primary priority and priority content. There is a further category called non-designated content (**"NDC"**) which was included in the Bill and subsequently the Act, which refers to content which presents a material risk of significant harm to an appreciable number of children in the UK, but which not captured by the other categories of content. There are specific duties on service providers to ensure that, in the event that a service provider finds content that could be harmful to children on their service while undertaking a risk assessment, but that does not fall into either primary priority or priority content, they still have duties to protect children from that content, as well as to notify Ofcom about the types and incidence of that content. In this way, the government wanted to future proof the duties and ensure they were as comprehensive as possible. Therefore, there were no specific categories of non-designated content that the government was aware of during this time. Where there was sufficient evidence of harm for a known category of content, this category was included as either primary priority content or priority content within the Act. The inclusion of non-designated content in the Act reflected the acknowledgement that additional categories of harmful content could arise in future, which were not specifically referenced in the Act.

General

123. In relation to online safety during the pandemic period, the focus of DCMS was on the Bill and taking the steps needed to ensure that there was regulatory change in future.

124. While the department's primary focus was on the Bill, additional regulatory interventions during this period provided interim safeguards for children online. Since

1 November 2020, UK-established video-sharing platforms (**"VSPs"**) have been required to take appropriate measures to protect children from videos containing restricted material, and all users from videos containing harmful material, including certain types of illegal content and incitement to violence or hatred **[EM8/49 - INQ000610354]**. Currently, although VSPs meet the definition of user-to-user services, which are regulated by the Act, they are exempt from the Act's safety duties during a transitional period. They will become subject to these duties when a provision in the Act repealing the VSP regime is brought into force, which is expected to be in Summer 2025.

125. The Age Appropriate Design Code contains 15 standards that the ICO or a court must take account of when considering whether online services have complied with their obligations under data protection law to safeguard children's data online. The Secretary of State laid the Age Appropriate Design Code before Parliament under section 125(1)(b) of the Data Protection Act 2018 on 11 June 2020. The Information Commissioner's Office (ICO) issued the code on 12 August 2020, and it came into force on 2 September 2020, with a 12-month transition period for industry compliance **[EM8/50 - INQ000610355]**.

126. DCMS worked with HO and the DfE to produce a resource page on gov.uk on child online safety **[EM8/46 - INQ000518754]**. This page was in response to an industry-led child online safety campaign, led by Microsoft and supported by social media companies. The Gov.uk page was linked in adverts and provided parents and children with existing online safety resources.

127. Following this publication, the department's analysis indicated that there was still a gap in guidance for parents and children on having productive conversations about online safety and which focused on legal but harmful content online. The government expected more people to be online as a result of lockdowns and other NPIs such as school closures which could expose users to higher levels of online harm, and this was a particular concern in relation to children. At the time, the DfE estimated that 98% of children were not in school and it considered there to be a greater risk to child online safety during this time. Information from law enforcement indicated that the CSEA threat had increased as a result of Covid-19 measures. Children's charities

also reported to DCMS increased reports from users on legal but harmful issues such as cyberbullying, concerns over children accessing inappropriate content, and children reporting significant rises in anxiety and stress.

128. As a consequence, a second set of guidance was published **[EM8/47 - INQ000518741]** which outlined a number of principles that users should take to stay safe online and covered a range of DCMS policy areas including online harms, data, cyber security, and disinformation. The guidance encouraged individuals to use technology to stay connected, while also encouraging individuals to consider the impact screen use is having on their wellbeing. In addition, DCMS engaged with government child safety policy leads across Whitehall to develop the proposed online safety guidance and ensure that related efforts taking place across government are signposted.

129. Following the release of this guidance, updates were made to the list of resources in the appendix to add other relevant organisations or sources of information which may have been helpful to the public. These were flagged by other government policy teams or at the request of stakeholders directly and reviewed by DCMS. I am not aware of any issues which arose which were not then reflected in changes to the guidance.

130. The guidance was launched with a press release, including quotes from high profile child safety organisations. The guidance had a proactive media package targeting national, regional and trade media with an interest in online harms and was also disseminated to key groups with parents and carers as an audience. Digital products to support the new guidance were also created and promoted online to relevant parents and stakeholders. For example, the content was adapted into a set of 'quick tips' for Mumsnet.

131. The guidance was intended to bring together information from a range of existing sources promoting online safety and wellbeing and had a reasonable level of engagement from the public. It was not intended to replace key ongoing work to address online safety through the response to the White Paper and other regulatory

interventions. Nor was it intended to replace the wider non-legislative work to develop a media literacy strategy to empower users, including parents, to safeguard themselves and their children online.

Section E - Post pandemic between 28 June 2022 to date

Mis and Disinformation

132. DSIT continues to draw upon its experience of the pandemic, and the challenges that arose at that time and subsequently, in its work on mis and disinformation. It also continues to recognise the vital importance of both responding to information threats and respecting freedom of expression.

133. In October 2023, Ministers changed the remit and name of the CDU. Its new remit was to tackle the greatest national security risks facing the UK from mis and disinformation, specifically looking at threats posed by foreign states, risks to elections and from the use of AI and deepfakes. The CDU was renamed the National Security and Online Information Team (**"NSOIT"**) to reflect the new remit more accurately.

134. The remit of the NSOIT is subject to ministerial agreement. Therefore, following the change of government in July 2024, the remit of NSOIT was amended to cover threats to public safety, as well as national security. While the remit of public safety does not mean that the NSOIT routinely looks at the information environment in respect of public health mis and disinformation, it does mean that if there was a public health crisis, for example a pandemic, NSOIT would have the remit to look at mis and disinformation in those circumstances.

135. NSOIT has worked to reduce reliance on external providers and improve analytical techniques, including through the development of the in-house Counter Disinformation Data Platform (**"CDDP"**). The objective of the CDDP is to provide a shared resource across government, enabling teams to bring their analysis in-house to lower security risks, further improve the anonymising of information and enhance the system's understanding of the threat in real time, particularly that posed by malign actors to UK audiences. The CDDP can be used by teams across government to

improve collective understanding of the mis and disinformation threat, enabling better preparedness for a mis or disinformation incident, improved sharing of data and consistency of analysis across government. As technology continues to develop in this area, DSIT periodically reviews the analytical tools it currently uses as well as alternatives on the market, considering their effectiveness in understanding online threats both now and in the future. DSIT is currently undertaking such a review.

136. NSOIT's focus is on the mis and disinformation itself rather than the author of the content or the specific parts of the UK audience who have viewed the content or at which it is aimed. Therefore, neither NSOIT or the CDDP is focused specifically on mis and disinformation which is aimed at children, or which children are likely to engage with. It is highly likely that some of the mis and disinformation trends and narratives which have been identified by NSOIT and/or the CDDP would have been viewed by children.

137. DSIT is also taking steps to address mis and disinformation where it constitutes illegal content or content which is harmful to children through the Act **[EM8/03 - INQ000642745]**. Under the Act, all companies subject to the safety duties must now take action against illegal content online, including mis and disinformation, and providers of user-to-user services are required to have in place systems to remove in-scope content from their platforms if they become aware of it. This includes the false communications offence, which came into force on 31 January 2024. As a result, it is an offence to spread information which a person knows to be false but still distributes it, with the aim of causing harm to anyone who views it. Also covered by these duties is content amounting to the foreign interference offence, created by the National Security Act 2023, which has been included as a priority offence in the Act, requiring companies to take action against a wide range of state sponsored mis and disinformation and state linked online interference.

Media Literacy

138. Between 2022 and 2025, DCMS, and subsequently DSIT, provided nearly £3 million in funding for various media literacy projects, including educational interventions designed to empower users to make safe and informed choices online. In total, 17 projects received funding through the Media Literacy Taskforce Fund and

the Media Literacy Programme Fund for at least part of the funding period. Of these projects, seven provided dedicated media literacy support to children and one specifically supported parents and carers. The projects provided broad media literacy support and were generally intended to help build resilience to a wide range of online harms. The funding criteria included a requirement for organisations to evaluate the impact of their projects, thereby helping to improve the evidence base of what works in media literacy interventions.

139. In 2024, £0.5 million in additional funding was provided to two of the organisations to scale up their programmes, which provide media literacy support to teachers, children aged 11-16, parents/carers and other professionals working with families.

140. Specifically, the National Literacy Trust received funding to expand their 'Empower' programme, which focuses on women's and girls' online experiences. It delivers media literacy education to students aged 11-16 attending alternative provision and trains schoolteachers to teach media literacy topics. In 2024-2025, the programme reached 3,746 students as part of 393 cohorts in 266 settings. According to the evaluation report, the number of students checking whether a news source was trustworthy increased from 34% to 74%. 89% of student participants reported that they now understood how different news companies present stories differently and 85% were now aware of how social media can affect their mental wellbeing. Furthermore, 94% of teachers who participated committed to integrate this content in future lessons.

141. Parent Zone received funding to expand their 'Everyday Digital' programme, which provides online resources and in-person training on media literacy for family-facing professionals, parents, and carers. In 2024-2025, the project reached 63,931 parents in 29 local authority areas. According to the evaluation report, parents gained practical skills in setting digital boundaries, identifying misinformation, and fostering open conversations at home. The initiative delivered a 45% increase in understanding of media literacy in the target group, a 25% increase in their confidence about media literacy risks and a 32% increase in their confidence discussing online safety and positivity with their children.

142. The Act **[EM8/03 - INQ000642745]** also updated Ofcom's statutory duty to promote and improve media literacy in relation to regulated services in several new areas. These duties are now in force and DSIT's media literacy team work closely with their counterparts in Ofcom on this issue.

143. Under the new media literacy duties, Ofcom is required to enhance public understanding of how to stay safe online. Ofcom must encourage the development and use of technologies that help users of regulated services to protect themselves. It must also raise awareness of the nature and impact of misinformation and disinformation, and help the public assess the reliability, accuracy and authenticity of content found on regulated services. It must help the public understand the nature and impact of harmful content and online behaviour, especially where this content or behaviour disproportionately affects certain groups, such as women and girls.

144. To meet these objectives, Ofcom is required to pursue media literacy activities and initiatives, commission or encourage other organisations to deliver such activities and initiatives and make arrangements for research to be carried out. Under the new duties, Ofcom must publish a media literacy strategy at least once every three years, setting out their objectives and priorities for that period. It must also publish an annual statement outlining progress against its strategy. Ofcom's first three-year strategy, 'A Positive Vision for Media Literacy' was published in October 2024. DSIT will work with Ofcom as it implements its strategy and has commissioned research to help target the next phase of DSIT's media literacy activity and ensure it complements Ofcom's efforts in complying with its duties under the Act.

145. The government has established an independent Curriculum and Assessment Review, which seeks to deliver a curriculum that readies young people for life and work by building the knowledge, skills and attributes needed which young people need in order to thrive. This includes digital skills. DSIT's media literacy stakeholders provided evidence in response to the Call for Evidence last autumn. The interim report, which was published in March 2025 **[EM8/51 - INQ000609984]**, noted that the rise of AI and trends in digital information require heightened media literacy and critical thinking skills. As set out in the interim report, the review will

focus on ensuring that the curriculum responds to social and technological change, including a renewed focus on media literacy, in its next phase of work. The review's final report and recommendations will be published in autumn 2025, along with the government's response.

146. Over the course of 2025, DSIT will collaborate with the DfE to consider the Independent Curriculum Review's recommendations and work to enhance media literacy education for young people. This includes leveraging research and insights from government-funded projects on best practice to develop effective approaches to improve media literacy skills of students, teachers, and parents.

147. DSIT also aims to embed media literacy across various cross-cutting government strategies, including Digital Inclusion, to boost online confidence and safety.

Online Safety

148. The Bill gained royal assent and the Act **[EM8/03 - INQ000642745]** became law in October 2023. The Act contains a range of measures intended to improve online safety in the UK and includes protections which have been designed specifically for children, with the aim of making the UK a safe place to be a child online. Companies with websites that are likely to be accessed by children need to take steps to protect children from harmful content and behaviour, and these duties are expected to come into effect from July 2025. For example, in-scope platforms will be required to have in place measures 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. The Act sets out categories of harmful content that platforms need to protect children from encountering, identifying that children must be prevented from accessing Primary Priority Content, such as pornography, and should have age-appropriate protections from Priority Content, such as content which depicts or encourages serious violence or injury. 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, [**EM8/52 INQ000610039]**, along with an additional impact assessment **[EM8/53 - INQ000610030]**.

149. Ofcom is now the independent regulator of the online safety regime, and the government is working with Ofcom to implement the Act. Ofcom is taking a phased approach to bringing duties into effect. The Act sets an 18-month timeframe for Ofcom to finalise certain guidance and codes of practice for illegal harms and child safety. Ofcom has met this deadline, and the illegal harms and protection of children codes were finalised and laid in parliament on 16 December 2024 and 24 April 2025, respectively.

150. Both DSIT and Ofcom are taking steps to implement the provisions of the Act. The draft illegal harms codes of practice and risk assessment guidance were finalised on 16 December 2024, at which point the draft codes were laid before Parliament. Furthermore, following the publication of the associated risk assessment guidance, services had until 16 March 2025 to complete illegal content risk assessments for their services. Additionally, Parliament has approved the draft codes, and the illegal harms duties are now fully in effect. This means that Ofcom can start enforcing the regime where platforms have failed to comply and it has already begun to enforce these duties. For example, in April 2025 Ofcom launched an ongoing investigation into a suicide discussion forum service, which it suspects may have breached the illegal content duties.

151. Ofcom published its protection of children consultation in May 2024, which closed in July 2024. In April 2025 Ofcom published Protection of Children Codes [**EM8/54 - INQ000609981**] Protection of Children Codes, which outline the steps that providers of in scope services can take to comply with the Act's child safety duties. In addition to publishing guidance alongside the codes on primary priority and priority content categories, which are mentioned above, Ofcom's codes also include types of content which could meet the definition of harmful NDC.

152. Ofcom published its finalised children's access assessments guidance on 16 January 2025 which helps services to determine whether they are likely to be accessed by children, following which services had three months to complete the children's access assessment process. Ofcom since finalised its Protection of Children Codes which were laid in parliament by the Secretary of State on 24 April 2025. Services likely

to be accessed by children have until 24 July to complete a children's risk assessment, to evaluate the risk of harmful content to children on their platforms. If Parliament approves the draft Protection of Children codes, the child safety regime will be fully in effect by summer 2025.

153. In its Protection of Children Codes, Ofcom has identified two kinds of content that meet the definition of NDC in the Act, because of the harm that may arise when this content is encountered in high volumes. These are 'content that promotes depression, hopelessness and despair' (depression content) and 'content that shames or otherwise stigmatises body types or physical features' (body stigma content).

154. DSIT has made no formal assessment of whether these harms were caused by, exacerbated by, or accelerated by the pandemic. However, some of this online content within these broad categories will have been produced prior to the pandemic.

155. Although DSIT has not conducted its own research into the effects of the pandemic on children's online lives, it has commissioned and published **[EM8/55 - INQ000609985]** some research since the pandemic on the impacts of online content on children. This includes reports delivered by NatCen, "content and activity that is harmful to children within scope of the Online Safety Bill" and Ecorys, "qualitative research project to investigate the impact of online harms on children" **[EM8/25 - INQ000609980] [EM8/56 - INQ000598443]**.

156. In addition, in November 2024 DSIT announced **[EM8/57 - INQ000610040]** a feasibility study on methods and data to understand the impact of smartphones and social media on children. The study ran for six months, and the final report will be published in due course.

157. In relation to planning for a future national emergency, DSIT has implemented key measures to maintain digital and online connectivity during national emergencies. These include enhancing the resilience of telecom networks, protecting digital infrastructure through cybersecurity legislation, and strengthening essential services

like the 999-emergency system. These efforts are designed to reduce service disruption, safeguard access for vulnerable groups, including children, and support the UK's wider emergency response strategy.

158. In addition, DSIT has outlined four key focus areas in its 2025 Digital Inclusion Action Plan: First Steps (**"the Action Plan"**) to ensure that everyone has the access, skills, support, and confidence to engage in our modern digital society and economy, whatever their circumstances. This will help to ensure that children can continue to access online services during national emergencies. The Action Plan recognises five demographic groups that are more likely to face barriers to digital inclusion. This includes low-income households, and young people, including those not in education, employment, or training. The Action Plan outlines four focus areas for future work:

a) **Tackling data and device poverty** - The Action Plan outlines the importance of having access to the internet and highlights initiatives like the National Databank, which has distributed over 125,000 free mobile data packages to help families stay connected. There is also a focus on ensuring everyone, including children, has access to appropriate devices (e.g., laptops or tablets) to continue their education and access essential services.

b) **Opening up opportunities through skills** - The Action Plan articulates that immediate action is needed to ensure that everyone should leave school with the right digital skills and commits to enhancing support for the framework that helps people and businesses get the essential skills they need to get online safely and with confidence. The Action Plan recognises that these essential skills are required to interact safely online. These digital and medial literacy skills are vital during an emergency.

c) **Breaking down barriers to digital services –** The Action Plan highlights the importance of inclusive digital services. DSIT is working to ensure that all Government digital services are easy to use and save people time. This will be vital during an emergency.

d) **Building confidence and supporting local delivery** - The Action Plan highlights best practice including the London Borough of Kensington and Chelsea Digital Inclusion Partnership that provided digital skills training, device access and support

through local libraries and community groups during the COVID pandemic. Partnerships and hubs like these are especially important during emergencies when home connectivity may be disrupted.

159. During a national emergency, such as a future pandemic, the Act will ensure that, when children access online services, the service providers which fall within its scope will have duties to protect children from harmful content as outline above. This differs significantly from the situation during the pandemic, when the regulatory regime was far more fragmented.

160. The Act also includes a provision which enables DSIT's Secretary of State to issue directions to Ofcom in specific circumstances: where there is a threat to public health or safety or a threat to national security. The directions given by the Secretary of State can take one of two forms:

a) a direction requiring Ofcom to exercise its media literacy functions in order to give priority to specific objectives for a specified period in order to address the threat or

b) a direction requiring Ofcom to give a public statement notice to either a specific online service provider or to the providers of those services more generally. A public statement notice requires an online provider to make a public statement, within a specified period, on the steps they are taking in relation to the threat.

161. The provision also enables Ofcom to require a provider of online services to provide it with any information it needs in order to respond to the threat. Although the provision is in force, it has to date not been used. However, it is intended to be an important tool for addressing online harm in future national emergencies.

162. New technologies develop at pace, making it hard to predict the future online environment during national emergencies. The Act is technology neutral and designed to address emerging harms through NDC provisions. It covers a wide range of offences, adapting as new harms arise. The early implementation stage limits our ability to

assess the Act's full impact. Despite this, the Act is expected to make a significant contribution, with HMG and Ofcom actively monitoring its impact over time.

163. However, it is clear that the Act provides far more protection to children and young people, than the regulatory regimes which were in place during the pandemic. Specifically, the Act's requirement for services to protect children from harmful content, including through the use of highly effective age assurance tools, will shield children from significant quantities of harmful content online, including types of content which may proliferate during national emergencies. Moreover, Ofcom's measures in its Protection of Children codes which recommend that companies filter harmful content out of child users' feeds will reduce the risk of children encountering harmful content online in the future. Additionally, by capturing a wide range of services within the scope of the Act, and by creating the category of harmful non-designated content, attempts have been made to future proof the Act, as different services, trends, and harms emerge in the future.

Section F - Lessons Learned

164. As explained above, in relation to its work on mis and disinformation, DSIT has looked to build on the work which was done during the pandemic, for example by refining its policies and ways of working and developing new tooling. This has been done as an alternative to carrying out a comprehensive lesson learned exercise, which would be less efficient, more time consuming and more likely to interfere with business as usual activities, such as dealing with Russian mis and disinformation following the invasion of Ukraine.

165. In relation to online safety policy more generally, the regulatory landscape has been transformed by the Act. The protections which the Act delivers will ensure that children can safely access online services. As more provisions of the Act continue to be implemented, the protections available for both children and the whole UK population will only increase. DSIT's focus has therefore been on the implementation of the Act, as this will bring significant improvements to the public's online interactions, rather than undertake a lessons learned exercise on the public's online experiences during the pandemic.

166. Going forward, section 178 of the Act requires the Secretary of State to review the effectiveness of the regime 2-5 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 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 of its truth.

Signed: **Personal Data**

Dated: 23/07/2025