

Stronger voices Ofcom's role in protecting women and girls online

Key messages

- Women and girls face disproportionately high risk of online harm, such as misogyny, harassment, image-based abuse, and tech-enabled domestic abuse—risks that are compounded by intersecting factors like race and disability.
- The UK's Online Safety Act (OSA) mandates Ofcom to address these harms, but their proposed guidance takes a cautious and non-binding approach, relying heavily on repurposed measures from child and illegal content protections rather than setting specific standards for women's safety.
- Ofcom proposes vague reporting and assessment measures, without providing any useful guidance on what harms to measure.
- Ofcom's failures to set clear standards will undermine platforms attempts to develop consistent approaches to safety by design, undermining accountability and limiting platforms' ability to act meaningfully on the guidance.

If the proposed framework is implemented, it may have no effect or even create problems by creating the illusion of safety. Ofcom should strengthen its regulatory stance by:

- 1. Setting comprehensive platform safety standards, and design risk metrics that platforms should track.
- 2. Creating accountability mechanisms e.g., fines, that encourage platforms to take a duty of care approach.
- 3. Establishing a permanent stakeholder group within Ofcom including women and girls from varying backgrounds to advise on safe design and standards.
- 4. Supporting a civil society 'red team' to identify online risks to women and girls.
- 5. Requiring platforms to block serial offenders from re-registering or migrating across platforms.

The <u>draft guidance on protecting women and girls online</u>, which is part of the process of implementing the Online Safety Act 2023, is open for consultation until 23 May.

1 Introduction

Women and girls face disproportionate and distinct risks to their safety in online spaces. On the heels of International Women's Day this past March, the UK government pledged to halve violence against women and girls over the next decade. This bold pledge was born out of the growing evidence of the risks to the safety of women and girls: on average, a woman is killed every three days in the UK. 1 Digital technologies play a key role by hosting and amplifying these risks. Plan International's 2020 report on Girls' and young women's experiences of online harassment, reported that across 22 surveyed countries, 58% of girls reported experiencing online harassment.² Of this 58%, 85% reported experiencing multiple forms of harassment. ³These findings alone don't capture the complexity of risks of online harm. As scholar Kimberlé Crenshaw has shown, policy responses that do not attend to the intersection of gender with race, class, disability, or sexuality risk leaving the most marginalised women unprotected. 4 Glitch, a charity that focuses on tech-facilitated gender-based violence, identified that posts about women are significantly more toxic than the average social media post. What's more, there are more toxic posts about black women than there are about other women.⁵ The harms women and girls face are therefore indisputable, and addressing such harms requires a considered approach that acknowledges the distinct risks faced by different groups of women.6

The Online Safety Act was one step towards addressing such harms. Since it was passed in 2023, Ofcom, the UK's communications services regulator, has been busy fulfilling its new duties. Section 54 of the Online Safety act mandates that:

'OFCOM must produce guidance for providers of [user-to-user] services which focuses on content and activity [...] which disproportionately affects women and girls.' (Online Safety Act, 2023, Section 54)

1

¹ Jess Phillips MP. (2025, March 6). *Government pledges to protect more women from violence*. GOV.UK. https://www.gov.uk/government/news/government-pledges-to-protect-more-women-from-violence

² 14,071 participants across 22 countries: Australia, Benin, Brazil, Canada, Colombia, Dominican Republic, Ecuador, Germany, Ghana, Guinea, India, Indonesia, Japan, Kenya, Netherlands, Nigeria, Norway, Philippines, Spain, Thailand, USA, Zambia

³ PLAN International. (2022). Free to be online? Girls' and young women's experiences of online harassment. PLAN International. https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-EN.pdf

⁴ Crenshaw, K. (1998). Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics. In Feminism and Politics. Oxford University Press.

⁵ GLITCH. (2023). Digital Misogynoir Report: Ending the dehumanising of Black women on social media. GLITCH. https://drive.google.com/file/d/13x4P2ANjhJkx3Qodd0E3owrXmkE-ZTVJ/view

⁶ See recommendation 3

This guidance may provide advice and examples of best practice for preventing, assessing and mitigating risks of harm to women and girls and in producing it, Ofcom is obliged to consult officials such as the Domestic Abuse Commissioner.

In February, Ofcom released its <u>draft guidance for "A safer life online for women and girls"</u>. The issue of women and girls' safety online is complex, so is the legislation meant to address it, and so are the regulatory requirements born out of the legislation. For those new to this topic, this brief will introduce Ofcom's role in producing guidance and codes for service providers, summarise the recent draft guidance for protecting women and girls online, and conclude with key areas for improvement.

2 Ofcom 'guidance' and 'codes of practice': regulatory context

Ofcom is required by the Online Safety Act (OSA) to produce codes and guidance to support service providers in fulfilling the duties set out in the Act. Though there are technical differences between 'codes' and 'guidance', they are often referred to interchangeably. Codes carry more 'hard-edged' obligations, whilst guidance, as the name indicates, has a more advisory function. There are limitations intrinsic to guidance related to the OSA, as 'there is no obligation in the Act allowing Ofcom to enforce against the contents of its guidance directly'. ⁷ That said, guidance cannot be dismissed outright by platforms. Both codes and guidance play important roles in reiterating duties and obligations set forth by the Act and ways of meeting those demands.

Because the OSA regime is based on these codes and guidance, rather than direct and detailed command and control regulation establishing new criminal offences, the release of these documents is closely followed. Thus far, three tranches of guidance have been released to the public at varying stages of completion. The <u>illegal content Codes of Practice</u> were released first and have since been finalised as of December 2024. These codes lay the groundwork by defining the remit of online illegal harms and the measures platforms need to adopt to respond to illegal harms. The second key release was guidance for protecting children online. As is implied, this guidance is meant to outline specific measures that service providers need to adopt to make online spaces safer for children. The final <u>Protection of Children Codes and Guidance</u> was

⁷ For more, view the Online Safety Act Network's <u>explainer on Codes, Guidance and the Status of Quasi-</u> Legislation

released in April 2025. The third tranche is the recent release of the <u>draft</u> <u>guidance on protecting women and girls online</u>, which is open for consultation until 23 May 2025.

The Act was explicit in obligating platforms to manage risks of harm from illegal content and activity and content and activity that is harmful to children:

- '(2) To achieve that purpose, this Act (among other things)
 - (a) imposes duties which, in broad terms, require providers of services regulated by this Act to identify, mitigate and manage the risks of harm (including risks which particularly affect individuals with a certain characteristic) from (i) illegal content and activity, and
 - (ii) content and activity that is harmful to children
 - (b) confers new functions and powers on the regulator, OFCOM.'

(Online Safety Act, 2023, Section 1.2)

But the Act is not as protective for women and girls as it is for children.⁸ Ofcom has taken a cautious approach, extending measures to protect women and girls only as far as they are covered by the remit of protections against harm from illegal content and activity, as well as harms to children online. As such, rather than creating new measures, measures are instead repurposed and repeated between codes and guidance. This cautious regulatory posture is one that has been critiqued from civil society throughout the different cycles of draft codes and guidance for illegal harms and children.^{9,10,11} The next section examines the structure of the draft guidance on protecting women and girls online.

⁸ The term 'women and girls' appears 6 times in the Act whilst 'children' appears 451 times.

⁹ Online Safety Act Network. (2025, January 15). Statement on Ofcom's Illegal Harms Code of Practice—Online Safety Act. Statement on Ofcom's Illegal Harms Code of Practice - Online Safety Act. https://www.onlinesafetyact.net/analysis/statement-on-ofcom-s-illegal-harms-code-of-practice/

¹⁰ 5rights. (2025, May 6). UK's regulator Ofcom launches the country's first Children's Online Safety Code. https://5rightsfoundation.com/uks-regulator-ofcom-launches-the-countrys-first-childrens-online-safety-code/

¹¹ NSPCC. (2024). Joint Statement: Ofcom's Approach to Keeping Children Safe Online. https://5rightsfoundation.com/wp-content/uploads/2024/09/Childrens-Coalition-Joint-Statement-on-the-Childrens-Safety-Duties-Code-of-Practice.pdf

3 Ofcom's approach to protecting women and girls: Draft guidance summary

The draft guidance cites research on the harms that women and girls face online which informed the selection of four focus areas:

- Online misogyny 'This describes the circulation or promotion of content that actively encourages or cements misogynistic ideas or behaviours.' (Ofcom, 2025, Section 1.10)
- Pile-ons and online harassment 'This describes cases where groups of coordinated perpetrators target a specific woman or girl, or groups of women and girls, often with abuse and threats of violence. While pile-ons can happen to any user, they often target women in public life, such as journalists and politicians.' (Ofcom, 2025, Section 1.10)
- Online domestic abuse 'This describes using technology for coercive and controlling behaviour in the context of an intimate relationship.' (Ofcom, 2025, Section 1.10)
- Image-based sexual abuse 'This refers to intimate image abuse (the nonconsensual sharing of intimate images) and cyberflashing (sending explicit images to someone without their consent).' (Ofcom, 2025, Section 1.10)

To address these harms, the guidance proposes a 'safety-by-design approach' which centres on nine actions across three categories:

Taking responsibility

- Action 1 Ensure governance and accountability processes address online gender-based harms
- Action 2 Conduct risk assessments that focus on harms to women and airls
- Action 3 Be transparent about women and girls' online safety

Preventing harm

- Action 4 Conduct abusability evaluations and product testing
- Action 5 Set safer defaults
- Action 6 Reduce the circulation of content depicting, promoting or encouraging online gender-based harms

Supporting women and girls

- Action 7 Give users better control over their experiences
- Action 8 Enable users who experience online gender-based harms to make reports
- Action 9 Take appropriate action when online gender-based harms occur (Ofcom, 2025, Section 1.14)

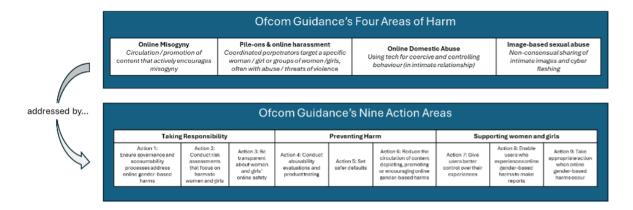


Figure 1 Ofcom. (2025). A Safer Life Online for Women and Girls: Practical Guidance for Tech Companies. https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/main-docs/annex-a-draftguidance.pdf?v=391669

For each action the guidance proposes 'foundational steps' and 'good practice steps' service providers can take to comply with their duties and go beyond.

- Foundational steps are 'measures providers can implement to meet their duties under the Act related to illegal content and protection of children. This information is taken from the Codes and risk assessment guidance [Ofcom] have set out across [their] work on illegal harms, protection of children, and (only as applicable to a smaller number of providers) transparency.' (Ofcom, 2025, Section 1.16, emphasis added)
- Good practice steps 'set out practical ways providers can go further to demonstrate a commitment to women and girls' safety.' (Ofcom, 2025, Section 1.17)

For example, take the foundational steps for 'Action 4: Conduct abusability evaluations and product testing':

- 'a) Product testing As a part of suitable and sufficient risk assessments (as outlined in Chapter
- 3), we have set out product testing as one of the types of evidence service providers could use as an input to improve the accuracy of their judgements on risk.
- b) Significant change risk assessment Service providers must carry out a new risk assessment before making a significant change to their service.
- c) Recommender system testing Service providers should, when carrying out existing onplatform testing of content recommender systems, collect additional safety metrics when making design adjustments, to evaluate whether the adjustment is likely to increase user exposure to illegal content.'

(Ofcom, 2025, Section 4.18)

In taking a cautious approach, the foundational steps are repurposed from relevant Codes' measures and risk assessment guidance already set out (Illegal Harms or Protection of Children). If service providers follow these steps, they will be compliant with their duties set out in the Act, but Ofcom does state that 'service providers may choose to comply with their duties in an alternative way that is more appropriate to their circumstances'. This caveat reveals the cautious nature of the guidance. Even steps which are meant to be foundational are made non-compulsory.

The additional 'good practice steps' would then include steps that, according to Ofcom, go beyond satisfying the basic duties set forth by the Act. As it pertains to Action 4, the good practice steps include:

- 'a) **User red teaming** for abusability testing, in which a product testing team takes on the role of a malicious actor and tries to attack a system in order to find vulnerabilities. This could be repeated periodically, even if there are no major developments, as perpetrators will adapt quickly to evade safety measures.
- b) **Working with experts** with direct or relevant experience engaging with and understanding perpetrator behaviours.
- c) **Using personas** to explore how different users may experience a feature and including intersectional perspectives.
- d) **Media literacy:** Adhering to the principles on monitoring and evaluating features in the <u>Best Practice Design Principles for Media Literacy</u>.'

(Ofcom, 2025, Section 4.20, emphasis added)

These steps are more ambitious and strike closer to directly addressing the four areas of harm. Yet, these 'good practice steps' are purely advisory. Such measures are often costly for service providers to adopt and without regulatory requirement, there is little incentive for platforms to adopt these measures proactively.

The research Ofcom included in this guidance is thorough, the harms it identifies are well justified, and the actions it proposes are sufficiently comprehensive. But the foundational and good practice steps are weak relative to the ambitions set forth in the Act, which aims to "make the use of internet services [...] safer for individuals in the United Kingdom" (Online Safety Act 2023, s 1.1). The excessive use of suggestive language ("could", "can") prominent in this guidance reflects this. The subsequent section will outline the key challenges of this draft guidance and specific recommendations.

¹² Ofcom. (2025). A Safer life online for women and girls: Guidance at a Glance. https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-on-draft-guidance-a-safer-life-online-for-women-and-girls/main-docs/guidance-at-a-glance.pdf?v=391670

4 Key challenges

This brief does not attempt a rigorous review of the various challenges this guidance faces but will instead focus on two critical areas for improvement: absence of standard setting, and a lack of safety by design for women.

4.1 Absence of standard setting

Ofcom needs to draw clear red lines by setting specific standards for service providers to work towards. The onus should not be on service providers to decide what is safe enough. This is evident in their Action 1 'Ensure governance and accountability processes address online gender-based harms' foundational steps:

'Board review: A provider's most senior governance body should carry out and record annual reviews of risk management activities in relation to online safety, and how developing risks are being monitored and managed.' (Ofcom, 2025, Section 3.11.a, highlighting added)

Codes of Conduct that set standards and expectations for individuals working for the providers around protecting users from online safety risks' (Ofcom, 2025, Section 3.11.f, highlighting added)

Despite spending an entire chapter identifying online misogyny, pile-ons and online harassment, online domestic abuse, and intimate-image abuse as the four areas of harm Ofcom seeks to address with its measures, the proposed measures fail to articulate what risks need to be managed and what standards need to be set in order to achieve progress in those areas of harm. This would have been an appropriate opportunity to make use of the extensive research on harms to inform the kinds of risks they expect platforms to be managing. However, the brevity and lack of specificity results in vague guidance that does not empower platforms to address their proposed harm areas. It is not sufficient to simply state that standards need to be set, the onus should be on the regulator to set such standards and decide what outcomes and results they want to see in relation to these areas of harm. This includes creating risk metrics for each harm area that can be used to track outcomes across different service providers.

Furthermore, the lack of clarity around what risks platforms should be managing also weakens its subsequent measures.

'Written statements of responsibilities for senior managers who make decisions related to the management of online safety risks.' (Ofcom, 2025, Section 3.11.c, highlighting added)

'Internal monitoring and assurance function to provide independent assurance that measures taken to mitigate and manage the risks of harm to individuals identified in the risk assessments are effective on an ongoing basis.' (Ofcom, 2025, Section 3.11.d, highlighting added)

The lack of specificity here raises the question as to what responsibilities senior managers can be assigned if it's not clear what risks regulators want them to manage. Whilst Ofcom is not empowered by the legislation to directly regulate according to standards, it is in a position to facilitate setting and monitoring of key industry standards as it is doing with age verification. Such monitoring and standards also facilitate transparency: the proposed guidance is weakened if service providers, users and the public are not given a sense of direction. Internal monitoring and assurance functions face a similar challenge. Industry needs clear rules and certainty, rather than vague language absent of proper standard setting.

4.2 Lack of safety by design for women

Although this guidance has the specific aim of reducing online risks for women and girls, the proposed measures are repurposed from the codes focused on illegal harms and on children. The guidance does not venture further than the previous codes and certainly does not require platforms to address harms for women. This is evident in Action 1 to 'ensure governance and accountability processes address online gender-based harms':

'Monitoring trends: Service providers should track evidence of new kinds of illegal content and content that is harmful to children on their services, and unusual increases in particular kinds of illegal content and content that is harmful to children (Ofcom, 2025, Section 3.11.e, highlighting added)

This measure lays out monitoring practices that should also extend to illegal content and content that is harmful to women as well. As one of the foundational steps for protecting women and girls from harm, this measure, and many of the other foundational steps, fail to extend protections to women. The following are a few more examples that demonstrate how permissive this guidance is in exposing women to risks that all people should be protected from:

'Negative feedback: Children can give negative feedback on content that is recommended to them by a content recommender system.' (Ofcom, 2025, p. 5.14.d,

highlighting added)

'Group chats: Children are given the option to accept or decline an invite to a group chat.' (Ofcom, 2025, p. 5.14.e, highlighting added)

'Take down: Content moderation function that allows the swift take down of illegal content and content harmful to children.' (Ofcom, 2025, p. 5.23.a, highlighting added) 'Signposting children to support when they search for harmful content, including suicide and eating disorder content. Provide children with crisis prevention information in response to search requests regarding suicide, self-harm and eating disorders.' (Ofcom, 2025, p. 4.37.f, highlighting added)

As these measures demonstrate, there are poor protections for women, but Ofcom has shown that they are able to extend a hardline standard:

'Recommender systems: Ensure that content that is likely to be harmful to children, including abuse on the basis of sex or gender reassignment, as well as content promoting gendered violence, is given a low degree of prominence on children's recommender feeds. Other kinds of harmful content – pornography, eating disorder content, self-harm and suicide content – should not appear on children's recommender feeds at all. Case study 11 includes further details on preventing children from encountering online misogyny.' (Ofcom, 2025, p. 4.37.b, highlighting added)

Unfortunately, this stance is only taken in relation to illegal content and activities, rather than harmful content and activities, and only for the benefit of children rather than other vulnerable groups.

One of the earliest stipulations of the Act is that 'services regulated by this Act are [...] safe by design' (Online Safety Act, 2023, Section 1.3), and these measures do not reflect a safety by design approach. A safety by design approach approach means putting harms protection at the heart of the design process, and thus far we can see that safety designs are only narrowly cater to a subset of platform users, ignoring the necessary protections for other vulnerable groups like women, and furthermore, focus too greatly on illegal content rather than harms more broadly. A safety by design approach is only possible if Ofcom sets clear standards and risk measures that will allow them to hold service providers accountable to ensuring a decline in the four identified areas of harm, for all those vulnerable to these harms.

¹³ eSafety Commissioner. (2024, September 25). Safety by Design. https://www.esafety.gov.au/industry/safety-by-design

Recommendations

The arguments presented emphasise the paramount importance of adopting a comprehensive safety by design framework to address online harms, particularly those targeting women and girls. Without clear standards, resources, and enforcement mechanisms spearheaded by Ofcom, these initiatives risk remaining fragmented and insufficient to combat online misogyny, pile-ons, harassment, domestic abuse, and intimate-image abuse. A robust regulatory framework is crucial to ensure these measures wield meaningful impact and effectively foster safer online spaces.

To address these challenges, the following policy recommendations outline key steps to create safer online platforms:

- Ofcom should set clear standards addressing the four areas of harms¹⁴ for service providers to abide by as a part of each action's 'foundational steps'. This would include specific risk metrics for each harm area as they relate to proposed reporting and assessment duties. These should cover, for example, account suspensions for serious and repeat offenders and expectations for victim support.
 - Big Tech companies have demonstrated significant influence over political processes, privacy erosion, and behavioural manipulation. While these harms are known, national regulatory frameworks often fail to ensure effective compliance due to jurisdictional fragmentation and lack of clarity. This highlights the need for specific, enforceable standards to address well-documented risks.¹⁵
- 2. Ofcom should create accountability mechanisms e.g., fines, that encourage platforms to take a duty of care approach. This would work in synergy with the first recommendation as it requires Ofcom develop a 'taxonomy of harms that the duty of care was intended to reduce or prevent. This could contain harms such as the bullying of children by other children or misogynistic abuse, which are harmful but not necessarily illegal' (Perrin & Woods, 2018).
 - <u>Carnegie UK's Harm Reduction Regulatory approach</u> articulates this governance model well. There are also related models for safety by design such as the LSE's Digital Futures <u>'Child Rights by Design'</u>

¹⁴ Online misogyny, pile-ons and online harassment, online domestic abuse and intimate-image abuse ¹⁵ Danesh, P., Yazdani, A. H., & Rahimi, L. (2022). Transnational Governance of the Digital Economy: Legal Approaches to Regulating Big Tech Companies and Ensuring Global Compliance. Legal Studies in Digital Age, 1(1), pp.27–38.

<u>approach</u> which centres a rights-based approach to designing platforms which can inform the development of regulation which encourages harm reduction outcomes.

- 3. Ofcom should convene a stakeholder group not only involving civil society organisations and experts but also women and girls who are everyday users of online platforms particularly those from marginalised backgrounds. This group should support Ofcom's ongoing deliberative work in this area by serving as permanent soundboard about safe design, contributing to standard setting.
 - This is an approach also supported by the EU's <u>The Digital Services</u>
 <u>Act</u> states that platforms should "conduct their risk assessments and
 design their risk mitigation measures" with involvement from a number
 of stakeholders, such as independent experts and civil society
 organizations (Articles 45-47).
 - There are a number of projects seeking to increase collaboration between civil society organizations and platforms, including <u>Forus</u> and the <u>CADE</u> project, that highlight the importance of these relationships.
- 4. Ofcom should make abusability testing a foundational step rather than a good practice step. It should resource the establishment of an independent individual civil society 'red team' to test for significant vulnerabilities that may endanger women and girls online.
 - Abusability testing entails 'reducing usability for some users in order to improve usability for most users'.¹⁶ These efforts must be guided by clear standards and risk measures set by Ofcom. This preventative measure embodies the ethos of safety by design and embodies a duty of care approach by encouraging the adoption of proactive measures to identify risks before they occur.
- Ofcom should require platforms to prevent serial perpetrators from reregistering on the same platform or migrating to other platforms in a crossplatform effort to continue harmful or illegal behaviour such as child sexual abuse.

¹⁶ Beers, A., Nguyễn, S., Sioson, M., Mayanja, M., Ionescu, M., Spiro, E., & Starbird, K. (2021). The Firestarting Troll, and Designing for Abusability. International AAAI Conference on Web and Social Media, Information Credibility & Alternative Realities in Troubled Democracies Workshop. https://par.nsf.gov/servlets/purl/10315351

14 Stronger voices: Ofcom's role in protecting women and girls online

- A small number of users are often responsible for a large amount of online gender-based harm, particularly in cases of co-ordinated harassment.¹⁷
- Evidence shows these users engage in repetitive and abusive behaviour which targets women, such as repeatedly posting the same sexually explicit content¹⁸.

¹⁷ Ofcom Stakeholder Workshop 2 on Women and Girls Online Safety, 19 November 2024.

¹⁸ 3 Wilson Center (Jankowicz, N., Hunchak, J., Pavliuc, A., Davies, C., Pierson, S. and Kaufmann, Z.), 2021. Malign Creativity: How gender, sex, and lies are weaponized against women online. [accessed 30 December 2024].

Author: Stephanie Thelwall

Stephanie Thelwall is a PhD researcher at the LSE's Department of Media and Communications focusing on the intersections of culture, media, democracy, and design.

A special thanks goes to Defne Aras, Madison Esmailbeigi, Mira Gillis, Ririko Hirase, Sara George and Damian Tambini for their sustained research efforts and commitment throughout the process—their contributions were especially constructive in shaping the final brief.

The author is also grateful to LSE students whose thoughtful engagement provided an important foundation for this work – Zayna Resley, Andri Ridhiani Putri, Byeongyeon Yi, Gillian Rawling, Ilana Melka, Jiayi Wu, Jihyun Choi, Marc Siegel-Fernandez, Odelia Kamhi, Remi Waxman, Vismaya Ashok, Wenxi Tian, Yun Jeung Lee, Yuyang Gao and Zainab Oyiza Sanni.



Ise.ac.uk/ media-and-communications



Department of Media and Communications

The London School Economics and Political Science Houghton Street London WC2A 2AE

Email: media@lse.ac.uk

The information in this brochure can be made available in alternative formats, on request. Please contact: media@lse.ac.uk.

The London School of Economics and Political Science is a School of the University of London. It is a charity and is incorporated in England as a company limited by guarantee under the Companies Acts (Reg. no 70577)

The School seeks to ensure that people are treated equitably, regardless of age, disability, race, nationality, ethnic or national origin, gender, religion, sexual orientation or personal circumstances