NPC CONSULTATION RESPONSE TO THE ONLINE HARMs WHITE PAPER

Grace Wyld, Alex Green, Tris Lumley

NPC welcomes the Government’s Online Harms White Paper. We broadly support the intention to establish a transparent and accountable regulator and a statutory duty of care, to develop technological solutions to mitigate risk, and to empower people to use the Internet safely. We believe these are crucial to building a better internet.

However online safety exists in the context of a rapidly changing technological and social environment. In defining harms, codes of practice, and regulatory frameworks, the proposed regulator must therefore adopt an approach of continuous development. This should include transparency and accountability of decision making, through continuous engagement and co-design with civil society, including charities and the communities they serve. Regrettably, the White Paper makes few references to the role of civil society and charities as part of the solution, which we believe must extend well beyond responding to this consultation alone.

In this consultation response we focus on keeping children safe online. We urge the government to:

1. **Build on what already exists**: Better education and empowerment are important to mitigate online harm, and there is already a great deal of good work being done by charities that should be invested in.

2. **View online harms across policy contexts**: It is limiting to view online safety in isolation. Online risks are inextricably linked to offline vulnerabilities, which are connected to socio-economic status and protected characteristics such as sexuality and gender.

3. **Establish a ‘What Works’ Network for Online Safety**: There is underinvestment into measurement and evaluation of what works in practice. In education, there is fragmentation and duplication of resources, compounded by a lack of evidence on the connection between offline and online vulnerabilities. We therefore propose the establishment of a network to measure the impact of online safety initiatives and share best practice.

Underpinning each of these should be continual consultation with civil society to contribute to the transparency and accountability of the proposed regulator. Charities and community groups are best placed to ensure the Government's strategy of empowerment of people and communities succeeds.

NPC is the independent think tank and consultancy for the social sector. Our mission is to help charities and their funders to optimise their impact, thereby supporting the people, places and causes at the frontline of social change. This gives us a very good feel for the barriers that hold charities and social enterprises back, and we work with them to co-design and develop solutions to overcome those barriers.

This consultation response builds on our 16 years of experience working with the social sector. As a think tank and innovation centre we are interested in harnessing the potential benefits of technology and data for those least likely to benefit from commercial tech products & services, such as our work with young people: My Best Life: Priorities for digital technology in the youth sector.
Build on existing initiatives for education and empowerment

We urge the government to build on effective, well evidenced initiatives to educate and empower people online already being undertaken by charities, rather than building something new. Interventions should centre around community resilience over individual education, and the government should encourage a more diverse pool of funding to allow the online safety sector to thrive.

1. Whilst the causes of online risk are often structural and systemic, education and empowerment are still crucial short-term approaches to mitigating harm online. The social sector already offers plenty of quality resources. For example, our forthcoming research with Nominet has identified over sixty initiatives operating in the UK for children, parents, carers, teachers and professionals, of which two thirds are focused on education and awareness.

2. The government should invest in effective interventions already operating in this space. For example, South West Grid for Learning and Childnet are charities working with schools and professionals to provide training and resources and to develop technical solutions, including a child-friendly search engine and school Internet services.

3. The Government should avoid seeking to educate individuals about specific platforms, and instead invest in interventions which develop community resilience and transferable skills. Platform-specific resources age rapidly – resources based specifically on Snapchat and Instagram will soon be as out of date as guides for platforms like Vine (closed 2017) or Bebo (closed 2013) would be today. A singular focus on individual education, while education is important, also neglects the important role that families and education professionals play in supporting safe Internet use.

4. We’ve found no shortage of resources. However, what’s there is fragmented and often duplicated. A lack of evidence (see below) means it is hard to know which interventions work best. Duplication of resources can lead to confusion and inaction for parents and professionals, so we recommend investment in coordinating resources, and careful targeting of any future government-funded media literacy initiatives to minimise duplication and waste.

5. Initiatives working to empower and educate people about online harm need a broader diversity of funding. Most initiatives in the sector are at least part funded by tech companies and internet service providers, which means they tend to focus on technical solutions, such as putting controls on devices. Partnerships between charities and the corporate sector can often lack focus on impact for beneficiaries, being driven instead by funding needs and desire to enhance brand or corporate reputation. We explored the root causes of this in our report Building more impactful corporate-charity partnerships. To address this, the Government can play a valuable role by brokering relationships, addressing power imbalances by funding charities to engage with online safety, and thinking carefully about how to engender meaningful cooperation between tech start-ups and community organisations.

View online harms across policy contexts

Online safety cannot be taken apart from related social policy areas, such as education and socio-economic status. There is underinvestment in understanding the evidence for how these factors link.

6. The Internet offers unrestricted access to a wide range of content, greater speeds and scales of interaction and a greater persistence of communication. This can extend and enhance individuals’ existing vulnerabilities, and expose new ones, even if such vulnerabilities are not obvious in the offline world.¹ Online harms are not experienced in isolation, but instead are situated in relation to online and offline social contexts, individual capabilities and forms of social and economic capital. The Government’s strategy for preventing online harm should therefore be viewed in a wider picture of social exclusion and policy.
7. Education is an important example of where online safety policy overlaps. The Government must improve schools’ ability to teach this topic. An estimated 40% of schools currently have no teacher training plans related to online safety. This lack of capacity within the education system has created a market for companies to sell one-off assemblies or class sessions, which are ineffective for building individual skills and creating the supportive school environments necessary for resilience.

Establish a ‘What Works’ Network for Online Safety

If the UK is to become a world leader in online safety, space must be carved out in the What Works network to invest in better evidence, communication and decision-making.

8. While there is a growing body of academic research literature relating to online harms, and valuable syntheses of research produced by UKCCIS, there is clear underinvestment into measurement and evaluation of interventions to prevent or mitigate harm. In the provision of educational materials for children, parents and carers, there are multiple resources addressing similar topics without a clear understanding of what works. There is also a lack of evidence on how offline vulnerabilities contribute to online vulnerability. We therefore propose the establishment of a What Works Network for Online Safety to bring together organisations developing online safety interventions with expert evaluators and academic researchers to improve the effectiveness of services and build a shared evidence base.

9. Alongside greater understanding of what works to improve online safety, more evidence is needed to understand whether specific risks lead to harm. Research studies have investigated harm in relation to some aspects of health, sexual behaviour and bullying, but there is limited evidence on privacy-related or economic harms, and ongoing debate on screen time, despite these being highlighted as significant concerns for children’s Internet use. There is also limited evidence about the prevalence of harms, with incidence rates derived from self-reported survey data showing great variability. For example, studies on cyber-bullying have reported rates ranging from 9% to 72%.

10. We do not know enough about the connection between online harm and socio-economic-status (SES) We do know that SES has a significant effect on how children use the Internet. Children from low SES homes tend to make less daily use of the Internet. They also report having significantly fewer digital skills than their better-off peers. In contrast, academic research has indicated that parents with higher SES tend to offer more forms of online support to their children and are more active in monitoring screen time. But whilst research has identified some trends in this area, further work is needed to fully understand the connections between SES and online harms.

Consult civil society meaningfully and continuously

The government should take a user centred approach, consulting and co-designing with people and communities affected by online harm, working with the charity sector to reach diverse communities and those who are most vulnerable online.

11. For people to be empowered to stay safe online, civil society should be meaningfully consulted and involved on an ongoing basis. Charities can act as an important conduit for government to speak to communities. Charities already working with children and young people are well placed to magnify their voices in the development of online safety provision. Charities also interact with parents, carers, teachers and other frontline professionals working with vulnerable people or children, whose views are crucial in the development of useful education resources and guidance.

12. People who are vulnerable to harm online are not sufficiently involved in service design. In the case of children and young people, most provision is shaped by the concerns of adults and focuses on restrictive
strategies which seek to avoid harm by reducing children’s online participation through staying off platforms or refraining from posting. If the people we’re trying to protect from harm are more involved in exploring and designing responses to staying safe online, we are more likely to be able to maximise the significant benefits the Internet has to offer.

13. There is a clear opportunity for the UK to establish itself as a world leader in online safety technologies. In growing this sector, government should enable and fund partnerships between tech companies and the social sector (especially youth centred and community organisations) to build on existing knowledge and community relationships. rather than starting from scratch. The proposed regulator should show leadership in this approach, involving civil society in the co-design of the codes of practice and guidelines.

Endnotes