NSPCC

Taming the Wild West Web

How to regulate social networks and keep children safe from abuse

EVERY CHILDHOOD IS WORTH FIGHTING FOR

Acknowledgements

Ahead of the Government's white paper on internet harms, the NSPCC have been assisted by Herbert Smith Freehills in developing a regulatory proposal that can protect children from the risks they face on social networks, including the risk of grooming and sexual abuse. We are hugely grateful to the team at Herbert Smith Freehills for their expertise. However, the proposals contained in this report represent the views of the NSPCC only.

In November 2018, the NSPCC held a roundtable to discuss the proposal with experts and representatives from social networks and the technology, regulatory and children's sectors. We are grateful for the considered and thoughtful contributions at the roundtable and in subsequent weeks.

Contents

1. Summary

For over a decade, social networks have repeatedly failed to protect children from abuse – and children have been placed at unacceptable risk. Most platforms have been cavalier when it comes to keeping children safe.

But there is finally the opportunity to put that right.

For too long, social media providers have been able to treat child safeguarding as an optional extra, not a necessity. Most platforms have failed to integrate adequate child protection measures into their business models or the design of their sites. The unwillingness of platforms to take the necessary steps has actively fuelled the scale and extent of the abuse risks that children face.

The NSPCC is clear that after a decade of inaction, it's time to introduce statutory regulation on social networks. Further self-regulation is a wholly inappropriate response to the unmanaged risks to which children are currently exposed. And it would mean the same sites that have comprehensively failed to protect children to date, through their failure to proactively tackle grooming, take down inappropriate content or do enough to tackle child sexual abuse imagery at source – would remain able to decide for themselves whether and how they protect their child users.

In the coming weeks, the Government has the opportunity to act. The Home Secretary Sajid Javid and the Culture Secretary Jeremy Wright will bring forward plans for legislation to tackle online harms, with the publication of an online harms white paper. This is a significant moment. Children deserve better protection than the status quo.

However, government will only deliver on its ambition to 'make Britain the safest place in the world to be online'[1] if it is bold and ambitious in its plans. If regulation is poorly devised, or not adequately built into law, children will continue to be put at risk.

Statutory regulation is the right solution to address clear market failure, and to prevent children from continued exposure to entirely unnecessary risks. Most other things that children consume – food, toys and clothes for example – all meet standards that let us know children are safe to use them. Social networks should not be the exception.

This report sets out the NSPCC's vision for a regulatory model that can keep children safe on social networks – and that places a legally enforceable duty of care on platforms to ensure their sites are safe for children to use.

Our regulatory approach envisages:

Strong and independent statutory regulation: statutory regulation is a necessary and proportionate response to the scale and extent of online harms. The regulator should be responsible for both content and behavioural harms, including technology-facilitated grooming. It should operate on a principles-based basis, and take a risk-based approach to its functions.

Platforms are subject to a legally enforceable duty of care: the regulator should require platforms to adhere to a legally enforceable, expansive duty of care that requires them to identify reasonably foreseeable risks. Sites must take steps at the system level to ensure its products and processes are both designed, and operated, in a way that minimises or eliminates children's exposure to them.

In the event that harm occurs, a platform would breach its duty of care if it failed to demonstrate sufficiently rigorous processes to identify or address it, or if children had been put in material harm as a direct result of how the site is designed or functions.

1 Department for Digital, Culture, Media and Sport (2017) Internet Safety Strategy Green Paper. London: DCMS.

Requirement to proactively tackle harms: platforms should be required to design and implement harm reduction strategies, targeting a list of harms set out by the regulator. They must also adopt a consistent set of minimum safeguarding standards, including a requirement to deploy proactive technology to tackle grooming.

Transparency and disclosure powers: at present, social media providers are able to selectively disclose what, if anything, they do to keep children safe on their platforms. The regulator should be given wide-ranging powers of information disclosure to build its understanding of the scale and extent of abuse risks that children face. Platforms should face new information disclosure duties, including a requirement to proactively disclose to the regulator any information it could reasonably expect to be informed about – and to 'red flag' cases to the regulator where their failings have resulted in a material breach in children's safety. In order to ensure a safety-by-design approach, sites should be required to undertake a risk assessment if they plan to introduce new services or amend their existing ones.

Compliance and enforcement powers: the regulator must be able to apply suitably robust enforcement powers to incentivise compliance. These should include the use of enforcement notices, and in the most serious cases, the ability to apply sanctions of a similar magnitude to the GDPR.[2] In cases where there has been a gross breach of a platform's duty of care, we propose that corporate criminal sanctions should apply. Platforms should be required to nominate a named director to be personally responsible for compliance, who should be subject to the personal risk of prosecution.

We now stand at a crossroads. The Government can decide whether it will introduce meaningful, enforceable change, or whether it will continue to let platforms decide for themselves whether to protect child users.

Our regulatory model rightly proposes that the platforms that create risk should be responsible for the costs of addressing it. For too long, children have paid the emotional, mental and physical costs of social networks failing to tackle abuse that is initiated and facilitated on their sites.[3]

It is time for the tech firms to be finally held accountable for the risks on their sites. It's time for the Government to adopt a robust regulatory approach and deliver for our children.

It's time to ensure every child is finally kept safe online.

2 GDPR fines can be 20 million euro or 4 per cent of global turnover, whichever is highest.
3 The Center for Humane Technology maintains a Ledger of Harms that lists 'the negative impacts of social media that do not show up on the balance sheet of companies, but on the balance sheets of society.'

2. Background

Why do we need social networks to be regulated?

Technology is central to children's lives. In 2019, just under half of children aged 12 had at least one social media account, despite the minimum age requirements for many sites being 13. By age 13, that figure rises to over two thirds. Social media is now a ubiquitous part of childhood, but alongside wonderful opportunities, it opens up an array of potential harms.[4]

For too long, social networks have been allowed to treat child safeguarding as an optional extra. As a result, we don't have the same protections in place online as offline, and children are left exposed to unacceptable risks, in the spaces where they socialise, learn and play.

After a decade of inaction, the challenge is now considerable, but not insurmountable. Most platforms have failed to integrate child safeguarding into their business models or the design of their sites. Rapidly developing technology creates new opportunities to initiate, maintain and escalate abuse. As a result, the scale and complexity of the online threat is growing.

This must change, and it can. As the debate about how to tackle online abuse intensifies, the NSPCC is clear that tough but proportionate regulation is the only solution.

What are the risks to children on social networks?

Children face a range of abuse risks online, from the production and distribution of child abuse images, to the harmful effects of exposure to inappropriate content, to the growing scale of grooming facilitated by social networks. Platforms provide new opportunities for groomers to initiate and maintain their abuse.[5]

With so many children using social networks, gaming and messaging sites, it means that today's children and young people are increasingly exposed to the threat of abuse or exploitation, from both adults and their peers. Groomers can use social networks to target significant numbers of children, and to move them from well-known open platforms to encrypted apps and hidden sites.

New types of technology, notably livestreaming, have provided new opportunities for abusers to control and coerce children into increasingly extreme forms of abuse.[6]

Social networks have consistently failed to address these problems – and it is clear that their unwillingness to do so has actively fuelled the scale and extent of the risks that children now face. Platforms have failed to build in adequate safeguarding protections, take steps to proactively tackle grooming, and to do enough to tackle child abuse imagery at source.

The extent of technology-facilitated abuse

For children subject to technology-facilitated abuse, the impact can be life-changing. Despite the common misconception that online abuse is less impactful, NSPCC research[7] has shown that the impact of 'online' and 'offline' abuse is the same, no matter how the abuse took place. This makes industry's reluctance to tackle online abuse even more disturbing.

As technology has provided new ways for offenders to commit abuse, the onus has been on social networks to do everything they can to make their platforms safer. Having comprehensively failed to do so, we can now see the consequences of their inaction.

4 Ofcom (2019) Children and Parents: media use and attitudes report. London: Ofcom.
5 National Crime Agency (2018) National Strategic Assessment of Serious and Organised Crime 2018. London: National Crime Agency.
6 We Protect (2018) Global Threat Assessment: working together to end the sexual exploitation of children online. London: WeProtect.
7 Hamilton-Giachitsis, C et al (2017) Everyone deserves to be happy and safe. London: NSPCC.

Technology-facilitated grooming has become a major challenge. Across the UK, in 2017/18 there were over 3,500 police-recorded offences for sexual communication with a child.[8] In England and Wales, 70 per cent of offences (where the data were recorded), took place on Facebook, Snapchat or Instagram. This is despite such sites, as the largest social networks, having considerable resources to tackle abuse occurring on their platforms.

In 2018, the Internet Watch Foundation identified 105,400 URLs containing *child sexual abuse imagery*, an increase of one-third from the previous year.[9] Social networks will argue that progress has been made in the removal of child abuse images; and while this is the case, industry has consistently failed to tackle the production of abuse imagery at its source. Once abuse has been photographed or filmed, or a child has been persuaded to share self-generated imagery, significant and long-lasting harm has already been done. Abusers use social networks to coerce and control children, manipulate them into sending photos or videos, or to perform sexual acts on livestreaming sites.

According to recent NSPCC research,[10] more than one in seven children aged 11-18 (15 per cent) have been asked to send *self-generated images and sexual messages*. Seven per cent of 11-16 year olds say they have shared a naked or semi-naked image of themselves.

In the largest ever survey conducted on online harms, undertaken by the NSPCC and LGfL Digisafe, an average of one child per primary school class has been sent or shown a naked or semi-naked image online by an adult.[11] Groomers are able to exploit the design of social networks, using friend and follower suggestions to infiltrate peer networks, and to establish contact with children that can quickly escalate into requests for sexual messages.

The director of vulnerabilities at the National Crime Agency (NCA), Will Kerr, has told the UK Parliament that 'there are thousands of children being unnecessarily exploited and abused because the tech sector has a significant responsibility and the ability to stop far more [abuse taking place] at source.'[12] The Home Office says that it estimates 80,000 adults in the UK poses a sexual threat to children online.[13]

The failure of self-regulation

Self-regulation has demonstrably failed to keep children using social networks safe from abuse. Since a voluntary Code of Practice was first proposed in the Byron Review[14] over ten years ago, social networks have been consistently unwilling to prioritise child protection measures. Instead, the platforms have been able to choose for themselves whether and how they protect their child users.

8 Based on an NSPCC FOI request sent to all police forces in England and Wales, and recorded crime statistics provided to the NSPCC by the Police Service of Northern Ireland and Police Scotland. In England, Wales and NI, the relevant offence is sexual communication with a child. In Scotland, the equivalent offence is communicating indecently with a child.
9 Internet Watch Foundation press release, January 2019.
10 NSPCC (2018) Net Aware research on file.
11 NSPCC (2018) Children sending and receiving sexual messages: a snapshot. London: NSPCC.
12 Comments in oral evidence to the Home Affairs Select Committee inquiry, Policing for the future', on 13 March 2018
13 Speech made by the Home Secretary Sajid Javid at the NSPCC, on 30 August 2018.
14 Byron, T. (2008) Safer children in a digital world: the report of the Byron Review. London: Department for Children, Schools and Families.

At present, regulation in this area comprises a patchwork of voluntary guidance and codes, developed by the industry at the UK, EU and international level.[15] Although commendable initiatives, these voluntary codes suffer from common failings: they lack precise rules and standards, usually lack effective monitoring and oversight mechanisms, have weak (if any) enforcement mechanisms, and consistently do not impose any sanctions on sites that don't comply.

Ahead of the forthcoming white paper, the Home Secretary Sajid Javid has said that how far Government legislates will be informed by the action and attitude that industry takes.[16] However, social networks can no longer be given the benefit of the doubt – and in any event, it is increasingly clear that the complex behaviour of offenders means that action can no longer be left to sites on either a voluntary or piecemeal basis.

There is a high level of concern about the risks of technological-assisted abuse, and a strong appetite for statutory regulation to address them. According to Ofcom and the Information Commissioner's Office,[17] online child exploitation is the issue of most concern to UK internet users (cited by 53 per cent of respondents.) Among internet users concerned about the impact of harmful interactions, 62 per cent were concerned about the risks of children being groomed online.

Whether it is groomers using multiple sites to escalate and conceal their abuse, or offenders using third-party apps to signpost to private WhatsApp groups where child abuse images are being readily shared, it is increasingly clear that we need a co-ordinated strategy – a 'whole system' response.

This can only be delivered through statutory regulation.

15 In its recent inquiry into screen use, the Commons Science and Technology Select Committee describes a 'standards lottery that does little to ensure that children are as safe as possible when they go online.' Science and Technology Committee (2019) Impact of social media and screen use on young people's health: Fourteenth report of session 2017-19.
16 Speech made by the Home Secretary Sajid Javid at the NSPCC, on 30 August 2018.
17 Ofcom and the Information Commissioner (2018) Internet Users' experience of harm online: summary of survey research.

3. Statutory regulation of social networks

It's clear that independent statutory regulation is necessary – continued self-regulation is a wholly insufficient response to the complex and growing abuse risks that children face.

A statutory regulator should have clearly defined powers and objectives, avenues for cooperation with civil society, government and law enforcement, and appropriate resources to exercise its powers effectively.

In some respects, this regulatory framework would be novel. No other country in the world has yet established a regulatory system for social networks that achieves what the proposed UK legislation is seeking. As such, this is a further opportunity for the UK Government to demonstrate its global leadership in respect of keeping children safe from abuse online.

However, this is not the first occasion that markets have matured to the point that it is clear that regulation is both necessary and desirable to protect the needs of vulnerable users.[18] In order to protect children, there must be a regulatory framework that creates backstop protections just as we see in other sectors.

Other things that children consume – food, toys and clothes for example – all meet standards that let us know children are safe to use them. Social networks should be the same.

Our regulatory approach

Social media providers are not un-regulatable.

A regulator is the right solution to address a clear failure by the market to prevent children being exposed to online harms. In developing a regulatory proposal, we have considered other regulatory models in the UK and EU to identify the essential characteristics of an effective regulatory regime, and to build a proposal that reflects existing legislative requirements.[19]

The NSPCC envisages a regulatory approach built around the following four pillars.

1. *Independent, robust statutory regulation*: statutory regulation is a necessary and proportionate response to the scale and extent of online harms. The regulator should be responsible for both content and behavioural harms, including technology-facilitated grooming. The regulator should be independent but cooperate closely with industry to secure its objectives.
2. *Social media providers should be subject to a legal duty of care*. Regulation should follow a duty of care approach, drawing on existing regulatory models to ensure existing and future sites are built to be safe by design. The duty of care would underpin the proposed regulatory framework, and provides a clear, broad-based and future-proof basis for regulation of social media providers.
3. *A principles-based approach to regulation is essential*. Given the wide variety of social networking sites, a principles-based approach will ensure regulation remains flexible and responsive to technological and market change. It also means the strategy for reducing harms sits with the firms best placed to develop context appropriate solutions: the platforms subject to the regulation.
4. *Regulatory outcomes should drive cultural change:* successful regulation should deliver compliance of the core regulatory requirements, but also deliver a cultural change across platforms that have previously been able to choose for themselves whether and how they protect children.[20]

18 For example, the Government has introduced or strengthened regulatory protections across a range of areas, including high-cost consumer credit and the rent-to-own hire purchase sector.
19 For example, the e-Commerce Directive and the Audio Visual Media Services Directive.
20 The Financial Conduct Authority's sourcebook on 'Treating Customers Fairly' is an excellent example of how regulation has been able to embed regulatory norms, and in doing so, drive cultural change in the often troubled retail banking sector.

Duty of care model

We strongly support a regulatory model that places a formal duty on social media providers to act in the best interests of child users, and to operate on the basis of having a 'duty of care' to protect them from online harms.[21] Our proposal draws heavily on the excellent work undertaken by Perrin and Woods.[22]

The duty of care model is built on the premise that social networks should be considered as essentially a public space, where children socialise, make friends and play. Social media providers should be seen as responsible for taking all reasonable steps to ensure their platforms are safe, just as similar requirements apply to the operators of the local playground, swimming pool or workplace. Parity of protection – that equivalent protections should apply in both online and offline spaces – forms the centre of the NSPCC's approach to online safety.[23]

The model draws heavily on health and safety regulation, which is premised on a general duty to ensure health and safety as far as is reasonably practicable – but which leaves it to individual companies to adopt a 'sensible and proportionate' approach to how they achieve it. The financial services regime is implemented through a set of principles-based requirements, such as the obligation to treat customers fairly, that can be implemented flexibly.

As Perrin and Woods argue, the duty of care is attractive precisely because it is broadly-based – it sets out the required outcome, to prevent harm to children, but it doesn't prescriptively regulate the detailed process for implementation. Given the breadth, complexity and rapid change of social media companies, this is not only desirable, it reflects the fact that more detailed regulatory requirements might not be possible – and almost certainly wouldn't be future-proof.

The benefit of applying an overarching duty of care is that it can capture and respond to a breadth of existing and evolving risks. Duties of care set out in law 40 years ago or more still work well – for example the duty of care from employers to their employees as set out in the Health and Safety at Work Act 1974, which still provides the basis for health and safety protections today.

Scope of duty of care

The duty of care should apply in an expansive sense – covering users of the site, but also harms resulting from its platform more widely. This means that platforms should be expected to address any reasonably foreseeable harms being facilitated on their site.

At its most simple, this means that if a child is being abused across multiple platforms (for example if a non-consensual image is being shared), sites should have to take action regardless of whether the child themselves has an account.

Given that very few harms are likely to occur on only one platform or app, it is essential that the duty of care applies broadly to ensure we can meaningfully tackle the wider ecosystem of risks that children face.

For example, if a child is being groomed on a social network, but subsequently migrated to an encrypted app or a livestreaming site, we need a regulatory model that can deliver a suitable 'whole system' response to this.

Similarly, when abusers have been able to readily access directory apps on Google's app store, and use these to find public groups on WhatsApp that openly host and share child abuse imagery, we need a regulatory model that is capable of responding to such a cross-platform threat.[24]

21 This builds on our initial proposals for platforms to have a regulatory duty to act in the best interests of children, as set out in the NSPCC's response to the DCMS Internet Safety Strategy (December 2017.)
22 Perrin, W and Woods, L (2019) Internet harm reduction: a proposal. Carnegie UK Trust: Dunfermline.
23 NSPCC (2016) Parity of protection: keeping children safe online and offline. London: NSPCC.
24 Investigated by AntiToxin Tech and findings shared with the Financial Times, December 2018.

The duty of care might sensibly be applied on a 'best endeavours' basis. While all platforms should reasonably be expected to adhere to a set of minimum safeguarding standards, the regulator should recognise that the expertise and resources available to a large site such as Facebook or Google are significantly different to those likely to be available to a start-up.[25]

As a minimum, this means the regulator should recognise that the ability of larger sites to identify reasonably foreseeable risks, and to commit engineering and operational resource to address them, will be significantly greater from smaller sites. This assessment of proportionality should inform the regulator's approach to compliance.

Under the duty of care model, firms would be required to ensure their sites are safe at a system level – that means ensuring that their products are safe or low risk by design.

In order to demonstrate compliance with the duty of care, a social media provider would need to demonstrate it had taken reasonable steps to ensure its products and processes are both designed, and operated, in a way that minimises the potential for exposure to harm.

In the event that harm occurs, a platform would be in breach of its regulatory requirements if it couldn't demonstrate that it had taken such steps to minimise them from happening – or if children had been materially harmed as a direct result of the design or functionality of their site.

Harm reduction strategy – a risk-based approach to regulation

We envisage that the regulator would take a risk-based approach to its responsibilities, specifically focussing on harm prevention– and in doing so, promoting regulatory outcomes that will make social networks safer for children. This should take the form of the harm reduction strategy set out by Perrin and Woods.

Our risk-based approach to implementation should enable platforms to focus on substantive compliance, and direct their resources towards tackling the most prominent harms on their sites. As such, this should be considered a purpose-driven, agile and focused approach to tackling and reducing harms.[26]

Harm reduction strategy

To comply with their regulatory responsibilities, we anticipate that platforms would be required to operate under an agreed programme of harm reduction, and subject to a regular reporting framework against it.

The regulator would be able to actively assess progress against identified harms; and it could instruct sites to take additional safety measures, or impose sanctions, if they fail to appropriately resource or deliver their harm reduction strategies.

25 The principle that a higher standard of care is expected from larger companies is established in case law. For example, the case of Thwaytes vs Sotheby's (2015) concerned an allegedly negligent valuation by Sotheby's of a Caravaggio painting. In giving its judgement, the High Court stressed that Sothebys, as a leading international auction house, was required to exercise a higher standard of skill and care than smaller and less specialist outfits.

26 This reflects the risk-based model advocated by Sparrow (2011) in which the regulator should exercise choices about which harms to focus on, and using the range of instruments available to it, should prioritise those harms that most impede the achievement of outcomes. Sparrow, M. (2011) The Regulatory Craft: controlling risks, solving problems, and managing compliance. Washington DC: Brookings Institution.

Such a harm reduction strategy requires a three-fold approach:

- the identification of harms against which children should be protected;
- the measurement of these harms on social media platforms, to create a baseline, and;
- an enforced programme of harm reduction, in which industry is required to develop and implement harm reduction strategies.

At this stage, the regulator would be responsible for assessing that these programmes are sufficiently robust, and it would undertake a regular re-assessment of the scale and extent of harms on regulated sites. This would allow it to decide on the progress made by companies, and in turn to determine if enforcement action may be required.

We anticipate that the regulator should have statutory responsibility to tackle the most pressing harms, which should as a minimum include technology-facilitated grooming; and the online production and distribution of child abuse imagery.

This approach has the benefit of providing clear direction to the regulator, and the platforms, about where their harm reduction strategies should be directed. The regulator should have a requirement to report to Parliament on its performance in reducing these most prominent of harms.

However, it should be for the regulator itself, in consultation with civil society and industry, to develop the complete list of harms that should be tackled. This will ensure the regulator is able to bring to bear its regulatory, market and technical understanding when developing its list of regulated harms. It will also ensure that it can review and amend this list, as part of its regulatory work planning exercises, for example in response to technological and market changes, or in response to the evolution of the threat landscape.

Precautionary principle

It will be important that any regulatory framework introduced by the Government is underpinned by robust evidence that demonstrates the necessity and proportionality of the measures being introduced – not least to minimise the risk of costly and time-consuming judicial review.

However, while there is clear evidence that social media platforms are facilitating technology-facilitated abuse, the evidence base continues to develop around wider potential harms. Given their inherent reluctance to share data, social media companies arguably frustrate the development of evidence-based understandings of the impact of children using their sites.[27] As a result, it is likely to prove impossible to fully understand the scale and extent of online harms until and unless a regulator exists and has the information disclosure powers to compel firms to disclose data to it.

It is therefore important the regulator is instructed to act on a precautionary basis – that if a platform can reasonably be considered to be causing harm to its child users, in the absence of a rigorous evidence base to demonstrate that it is definitively not harmful, it is legitimate to act to regulate it.

27 For example, in its recent inquiry into the impacts of screen use, the Commons Science and Technology Committee warned that a lack of data from social media platforms is 'holding back the development of the evidence base'. In his oral evidence to the inquiry, Professor Andrew Przybylski of the Oxford Internet Institute described a 'fundamental informational asymmetry between industry researchers and academic scientists.

4. Minimum safeguarding standards – securing safety by design

The regulator should prioritise the principle of 'safety-by-design', through requiring social media providers to adopt minimum safeguarding standards for children and young people. This could potentially take the form of a legally enforceable 'safety-by-design' Code of Practice.

Platforms should be required to introduce these minimum safeguarding standards – and if they fail to implement these appropriately, could reasonably be considered to be failing to make their platforms safe.

As a result, they would be failing in their duty of care.

These accounts would offer a series of basic protections for children and young people – in effect creating 'safe accounts' for children. Although the precise scope of these standards should be determined by the regulator, in consultation with industry, civil society and children's experts, as a minimum the NSPCC considers these standards should include:

- default high privacy and account settings for children;
- clear and robust community standards
- transparent and effective reporting and complaints handling, and;
- proactive steps to prevent exposure to illegal behaviour, including grooming.

Default privacy and account settings for children

Children should have the **highest privacy settings** applied to their accounts by default, including: geolocation settings being turned off; contact details being private and unsearachable; children's accounts receiving regular prompts about their privacy settings; and livestreaming and chat functionality being restricted to users' approved contacts.

Children should not have to 'opt-in' to the highest privacy settings, and changes to settings should never be made without the express agreement of the account holders.

Children opening social media accounts must be made aware of the implications of joining, benefit from **accessible terms and conditions**, and understand what information other users will be able to access about them.

Children should be able to **livestream** only to their approved contacts; and platforms should be made introduce real time moderation and use algorithms to detect nudity and other behaviours that may place children at risk.

The regulator should explore options for how best to apply minimum safeguarding settings, including through the use of 'know your user' data. Alternatively, social media providers could assume all users are under 18, until and unless they can demonstrate otherwise. This approach to **account verification** would ensure all users are automatically given the safest possible set of features online.

Clear and robust community standards

Social networks should adopt **clear and consistent definitions of acceptable behaviour**, with a common understanding and consistent threshold for what constitutes abusive and harmful conduct. Policies should be expressed in plain language that is suitable for a child, and presented in accessible and easy to use formats.

Child accounts must be developed with **clear moderation practices** that prevent children from being exposed to harmful content. These processes may require a referral to law enforcement.

Steps should be taken to **prevent access to inappropriate content**, with social media providers ensuring that inappropriate, violent or adult content is either blocked, or placed behind age gates or interstitial warnings. Users should be encouraged to report inappropriate content.

Transparent and effective response to complaints

Clear and visible reporting processes: platforms should have a clear and visible reporting process, with regular prompts that explain to users how to report concerns and the reasons for reporting. Processes should be straightforward, easy to use and presented in suitable language for a child or young person to understand.

Separate reporting flow: Any complaint made by a child user or involving child abuse should have a dedicated reporting procedure, and should be escalated to a trained child safeguarding moderator, on an expedited basis.

Transparent and timely processes to respond: All social media providers should have clear timescales to handle and respond to reports and they should provide information at the point of complaint, in language appropriate to the user, about how reports will be dealt with.

Proactive steps to prevent exposure to illegal behaviour, including grooming

Platforms must be required to tackle harmful harmful and illegal behaviour, including grooming. There should be a regulatory requirement on firms to invest in measures to identify and prevent grooming taking place in their sites.

Specifically sites should be required to introduce algorithims to proactively identify and flag accounts displaying suspicious patterns of behaviour. Such analysis can be conducted in a non-intrusive way, using metadata to flag accounts which should be reviewed by moderators, and through the expanded use of artificial intelligence.

For example, metadata analysis can identify users making disproportionately high numbers of contact requests to children and young people, where a high number of contact requests to children are rejected, and where there is no clear familial or geographic underpinning to the requests.

Platforms have resisted attempts to introduce such measures proactively, or have failed to adequately set out what they do to proactively prevent grooming taking place. This is a choice they have made. There is no legal or regulatory impediment that prevents them from doing so – the European Commission has said that sites taking proactive steps to prevent inappropriate content should not be regarded as assuming liability for it.[28]

Duty to notify other platforms of content removal

Given the complex ecosystem of social media sites, harms can spread from one site to another rapidly. In order to counter such a rapid flow of harms, there is merit in exploring imposing a duty on platforms to track when inappropriate content they have designated suitable for deletion is shared more widely, through tools which allow content to be shared across multiple platforms. For example, the 'Share Post' functionality on Instagram allows instant reposts to Twitter, Tumblr and Facebook.

A duty for platforms to notify other platforms of such posts would enable social media providers to play their part in combatting the way in which harms can spread through the ecosystem. A corresponding duty could be placed on platforms receiving such reports to promptly assess and take action in response.

28 European Commission (2017) Communication on Tackling Illegal Content Online.

5. Regulatory scope

Our regulatory model should apply to all social media providers that make their services available to UK children. This should include any platform that could reasonably be used for social networking purposes, even if they were not primarily created for such purposes.

This functional model mirrors the financial services regime, in which firms become subject to regulation if they undertake one or more 'regulated activities'.

We would consider a platform to be subject to regulation if it demonstrates the following characteristics:

- It acts as a commercial provider;
- provides online services to UK users through a website, app or similar functionality;
- has the majority of its content created by users; and
- facilitates social networking functions, messaging or comments, and encourages interaction between users.

This definition would include sites like Snapchat, which has consistently refused to identify as a social network (it self-identifies as a camera company). It would also include gaming platforms such as Twitch.[29]

Regulation should capture any social network operating in the UK that offers its services to children, regardless of the size of its user base.

In the same way that food safety legislation must apply equally to the local sandwich shop and the largest supermarket chain, it is essential that children receive a consistent set of minimum protections, regardless of the social networks they use.

We have given careful consideration to whether platforms should be subject to regulatory requirements only once they reach a de minimis user threshold. However, this presents a clear risk that offenders might actively migrate to newer or smaller platforms, precisely because they have not (yet) been required to adopt minimum child safety protections. This unintended consequence could potentially place children using such smaller sites at increased risk.

We therefore propose that, while all sites serving UK children must be required to comply with the legislation, new platforms should have a grace period to do so. Platforms which fall within the definition of a qualifying social media provider would be legally required to notify the regulator after they have been operating for a 3 month period.

Companies would then have a further period, most likely between 9 and 12 months, to implement a phased approach to compliance.

Tiered approach to regulation

There is merit in considering a tiered approach to regulatory requirements, based on platform size, assessment of platform risk, and crucially, risks associated with its functionality.

While we envisage all social media providers would be required to adopt the minimum safeguarding standards set out in section 4, sites should be required to adopt any additional measures only where it is proportionate and necessary to address the risks associated with them.

Additional regulatory requirements should be considered on functionality types that carry particular risks, for example livestreaming sites. NSPCC research has demonstrated that the live, visual and unpredictable nature of livestreaming apps present clear risks for children and young people. Both primary and secondary aged children are at significant risk of being asked to perform sexual acts when using such sites, such as being asked to remove their clothes.[30]

29 Specific exemptions would apply for any platforms that could demonstrate to the regulator they had arrangements to prevent children and young people using their sites; blogs; digital news sites where social networking could be considered ancillary to the site's primary purpose; and 'limited network' sites that are only available to closed groups e.g. social networks only available to specific employers or employees.

30 NSPCC (2018) Livestreaming and Video chatting: a snapshot.

In adopting a risk-based approach, it would be desirable for the regulator to require sites with livestreaming functionality to adopt specific safety features for child users. It would also be appropriate for the regulator to require enhanced reporting on the nature of risks where it articulates specific concerns and the mitigation strategies that social media providers put in place to address them.

App stores

62 per cent of children aged 8 to 11 and 93 per cent of children aged 12 to 15 regularly use a smartphone.[31] This means that the two main app stores, run by Google and Apple, are important intermediaries through which children access social network apps.

Both app stores have policies to determine whether they make apps available for download. While neither Apple nor Google make these policies publicly available, Apple has previously removed a number of apps from its App Store[32] and has significant scope to determine which apps children are able to use.

Given their intermediary status, we see merit in considering how app stores should interact with the regulator. As a minimum, app stores should be subject to the regulator's information disclosure powers and required to as required with its investigations.

Further consideration should be given to how app stores could play an expanded role in protecting children, including whether wider regulation could be expanded to cover their functions.

31 Ofcom (2019) Children and Parents: media use and attitudes report. London: Ofcom.
32 For example, the Sarahah app was removed from Apple's AppStore in February 2018.

6. Transparency and disclosure powers

For over a decade, social media companies have been able to selectively disclose what, if anything, they do to keep children safe on their platforms. There is no requirement for firms to disclose the scale and extent of abuse risks on their sites. Larger platforms have issued their own transparency reports that provide barely any information about the risks to which children are exposed, and no information at all about the scale and extent of risks faced by UK children specifically.

In order to change this, the regulator must be given wide-ranging and comprehensive powers to require information disclosure. Platforms should be required to disclose any information that the regulator considers necessary, either to assist with its investigations or ongoing work.

Platforms should be made to publish annual transparency reports, and to comply with duties to:

- proactively disclose information to the regulator where children's safety is materially breached;
- conduct a risk assessment, if it plans to launch a new product or service, to assess the potential risks to children and set out the steps taken to minimise them; and
- proactively notify the regulator of any aspect it might be reasonably expected to be aware of, including any changes to how a platform protects and supports its child users.

Annual transparency reports

Transparency reports must be a key part of the regulatory solution, allowing the regulator, civil society and users to fully understand industry processes and hold them to account. This should also support a 'race to the top'.

As a minimum, regulatory reporting should set out how sites resource their moderation and reporting processes; the type and number of reports it receives; and the specific outcomes that result from reports made by children or in relation to child abuse.

Platforms should also report on the demographic usage of their sites, including a breakdown of the usage of specific apps and features by children.

Information disclosure powers

The regulator should have powers to access any information that it considers necessary to conduct effective investigations and support its ongoing work.

This must include the ability to compel social media providers to disclose information on an ad hoc or 'on demand' basis, where this information relates to serious breaches of child safety, is considered necessary for investigative purposes, or it will assist the regulator to assess the impact of apps or features against its specified list of harms.

Proactive duty on platforms to disclose

Platforms should be subject to a general proactive duty to disclose information to the regulator that it could reasonably be expected to be informed about. This would likely act as a useful means of regulatory intelligence-gathering – and is likely to be a useful way of embedding regulatory compliance into the business practices of sites.

Although potentially broad, its scope could be drawn with sufficient clarity that social media providers can properly understand the duty. In doing so, this would ensure the regulator is not inundated with (and platforms are not bombarded by) unmanageable volumes of unhelpful reporting.

A similar proactive duty already applies in the financial services sector. Principle 11 of the financial services regime requires firms to deal cooperatively with the regulator and to disclose anything of which the regulator would reasonably expect notice. This is supported by a non-exhaustive list of examples.

‘Red flag’ reporting where children’s safety is materially compromised

At present, there is no requirement for platforms to report in the event of significant lapses in children’s safety or a material breach in safeguarding. However, comparative reporting is widely used in other regulated settings.[33]

In November 2018, Apple took the decision to remove Tumblr from its app store after child sexual abuse imagery was found on the app. While it is reasonable to assume that this incident must have been sufficiently serious to justify the app’s removal, neither company was required to notify any external agency, there was limited public information about the scale and extent of the safeguarding lapse – and it is unclear what, if any, platform or wider systemic lessons might need to and have been learnt.

Platforms should no longer be able to self-police in this way. We therefore propose that platforms be subject to ‘red flag’ reporting. This requires immediate disclosure to the regulator in cases where the safety or wellbeing of children has been compromised or put at risk, or where there has been a material breach in child safety processes –cases where a platform has failed to adequately deliver its statutory duty of care.

Duty to conduct impact assessments on new services

Platforms should be required to conduct impact assessments before launching new product functionality or services, and to share these with the regulator prior to services being launched in the UK.

Impact assessments should specifically consider the potential impacts of services on children – and should enable a social media provider to demonstrate to the regulator that it has taken all appropriate measures to assess and mitigate against the potential risks of children and young people using the product.

This measure would encourage companies to constructively assess the impact of their services prior to them being launched. It would also allow the regulator to be appraised as the market changes and work with social media companies to drive best practice, rather than having to react to new product launches.

33 For example, financial services companies are required to make reporting disclosures under the anti-money laundering and financial services regime, and licensed gambling firms must report breaches against self-exclusion protocols.

7. Investigation, compliance and enforcement powers

Any regulator must meaningfully be able to hold non-compliant sites to account. In order to effectively regulate such large social media providers, the regulator will need intelligently-designed powers, and to be appropriately resourced to ensure compliance.

While there are examples of highly successful regulatory models, including Ofcom and the Financial Conduct Authority, there are also multiple examples of suboptimal regulatory design. For example, the asymmetry between the Information Commissioner's information disclosure powers and the large tech firms they regulate in respect of data protection; or Ofgem's poorly implemented disclosure functions that resulted in protracted difficulty in extrapolating the retail margins of the Big Six energy firms.[34]

This section sets out our proposals for the regulator to investigate platforms, and in the event of non-compliance, to impose appropriate enforcement measures.

Investigatory powers

The regulator should have robust powers to investigate platforms for non-compliance, and in specific cases where they have failed to address or respond to serious examples of harm.

In line with the powers available to other regulators, these should include the powers to:

- request or require any information which is necessary to assist the investigation, with penalties for a failure to cooperate or if sites provide inaccurate or misleading information;
- inspect premises and / or take possession of physical or electronic documentation;
- order participants to carry out research or impact studies (as is required in the tobacco sector) or to conduct internal investigations (as is required under the financial services and anti-money laundering regimes.)

Enforcement measures

As one of the largest markets for many social media providers, we anticipate that the majority of platforms will choose to comply with appropriately balanced but robust regulatory requirements.

For example, in Germany, the prospect of a significant sanctions regime led YouTube, Google and Twitter to meet their legal requirements to takedown illegal hate speech content in more than 90 per cent of cases in the first six months of the country's new NetzDG regulation.[35]

However, as Perrin and Woods have powerfully argued, any sanctions regime must be proportionate to the scale at which these companies operate.[36] Given the size and scale of social network providers, that means that the magnitude of financial sanctions and wider enforcement measures must be significant.

Furthermore, the regulator must have sufficient powers to incentivise behavioural change in companies that might otherwise be minded to breach their requirements.[37] At its most simple, enforcement measures must include sufficient penalties that it is not simply easier for a platform

34 Ofgem introduced a regulatory requirement for the Big Six to self-disclose their costs and retail margins from 2009, but came under heavy criticism because these were deemed to be ineffective in increasing the transparency and comparability of company profits. Commons Energy and Climate Change Committee (2013) Energy prices, profits and poverty: fifth report of session 2013-14.

35 The NetzDG legislation allows for sanctions of up to 50 million euro to be levied on platforms that fail to block or remove content that is 'manifestly unlawful' within 24 hours of a report being made. YouTube and Google removed 93 per cent of content within these timeframes and Twitter 98 per cent. Facebook actioned 76 per cent of content. Gollatsz, K et al (2018) Removal of Hate speech in numbers: LSE Media Policy Project blog.

36 Evidence provided to the Lords Communications Committee form its ongoing inquiry: 'The Internet: to regulate or not to regulate?'

37 Legal Services Board (2013) Overseeing regulation: the LSB'a approach to its role.

to 'pay the fine' and carry on with commercially advantageous but potentially harmful practices.

We therefore propose that the regulator has powers to apply the following civil measures.

Financial sanctions: The regulator should be able to levy financial sanctions where there is a breach of the platform's duty of care, or in circumstances where a platform fails to cooperate with the regulator or is considered to have provided misleading information to it.

Financial penalties must be of sufficient magnitude to deter non-compliance, and to eliminate any financial gain or benefit from a platform's decision not to comply with its regulatory requirements in the first place.[38]

For the most significant regulatory breaches, for example a platform that consistently fails to deliver against its statutory duty of care, there would be merit in adopting a sanctions regime with a similar magnitude to the GDPR i.e. up to 20 million euro, or 4 per cent of annual global turnover, whichever is higher.

The regulator should credit timely disclosure of regulatory breaches and reduce financial penalties accordingly.

Enforcement warnings and notices: the regulator should be able to direct sites to apply remedial measures in respect of children's safety, for example requiring the adoption of specified safety-by-design features.

Business restrictions or prohibitions: the regulator should be able to prohibit the continuation of certain activities, for example restricting the use of certain features.

Public censure and adverse publicity orders: This could include media campaigns or the use of orders whereby the platform is required to display a message on its homescreen setting out the details of how its actions placed children at risk. Similar adverse publicity notices are also used in Health and Safety regulation, for example through the use of publicity orders giving details of corporate manslaughter and negligence convictions.[39]

According to research conducted by PA Consulting, publicising regulatory breaches and enforcement action is an important way of building regulatory awareness and trust – and so could potentially support parents in being better informed about the potential risks posed by sites. This research shows that consumers feel more protected when they've heard of the regulator (82 per cent) and when any regulatory breaches are publicised (80 per cent.)[40]

Corporate responsibility

We consider that criminal sanctions should apply in respect of a social media provider that commits a gross breach of its duty of care. Such offences would be reasonable, proportionate and clearly linked to our regulatory objectives.

Other regulated sectors already make provision for corporate criminal sanctions to apply in the event that there are significant, system-level deficiencies – in essence, where a corporate entity fails to have sufficient controls and processes in place to prevent either criminality or harm.

For example, there are strict 'failure to prevent' offences, including the Corporate Criminal Offences set out in the Criminal Finance Act 2017. Under this offence, a company can be found liable for bribery or tax evasion offences, if it is unable to show it has sufficient processes in place to have prevented staff from committing an initial offence.

38 As recommended by the Macrory Review of Regulatory Penalties (2006), led by Professor Richard Macrory.
39 This relates to offences under the Corporate Manslaughter and Corporate Homicide Act (2007). Seward, K. (2009) Corporate negligence: top of the agenda. Thomson Reuters Practical Law.
40 PA Consulting (2018) Re-thinking Regulators: From watchdogs of industry to champions of the public.

An offence of Corporate Manslaughter may be committed where failings by an organisation's senior management are a substantial element in any breach of the duty of care that it owes to either employees or members of the public, and these result in death.[41] Criminal charges can be brought where there are repeated and persistent breaches under the Health and Safety Act 1974.

There is merit in exploring options for corporate criminal offences where a social media provider grossly fails to discharge its duty of care, and as a result of the platform not being made safe at the system level for children to use, children come to material harm.[42]

In such cases, if a court found that the platform had failed to introduce procedures or that these were not adequate, it could determine that this constituted a gross breach of its duty of care, and this could result in a corporate conviction.

While we anticipate that charges would only occur in extreme situations, we consider that the extension of corporate criminal offences will help to embed regulatory compliance at the highest levels – and it would publicly underline the severity of a platform that didn't take seriously its duty of care.

Director-level responsibility

There is a clear benefit in ensuring that responsibility for regulatory compliance is held at the most senior levels of social media companies.

We therefore propose that platforms are required to appoint a named director[43] who is personally liable for ensuring that the duty of care is upheld – with consequences for failing to address foreseeable risks and to ensure their platforms had appropriate polices and protections to deal with them.

Under existing legislation, individual directors can be found criminally liable for the consequences of failing to uphold a duty of care.[44] We favour the adoption of powers to disqualify directors that fail to uphold their responsibilities. In the event that a platform materially failed to adhere to its regulatory requirements, including a breach of its Duty of Care, the named director should therefore be subject to potential disbarring. This would be achieved through an offence being committed under the Company Directors Disqualification Act, and would require minimal amendments to the existing legislation.

The Government might also wish to explore means to secure compliance more deeply into corporate structures. Existing models work well in other regulated sectors, for example the Personal Licensing Model in the gambling regime, although there are legal and regulatory challenges in establishing a similar model in this sector.

41 Health and Safety Executive Guidance: Leading Health and Safety at work (Legislation). Accessed January 2018.

42 Given such offences would relate to a failure to discharge its legal duties to ensure platforms were fundamentally safe to use, rather than implying direct liability for the liability of content, we consider this would be consistent with the e-Commerce directive, which grants platforms 'safe harbours' from criminal prosecution to the extent they play a passive role in the hosting, transmission or catching of unlawful material.

43 A Director serving as an Executive on the company Board.

44 For example, named directors can be prosecuted under the common law offence of gross negligence manslaughter; and under section 33 of the Health and Safety Act 1974, a director can be found liable for a criminal offence that is attributable to their neglect.

8. Working effectively with civil society, regulators and industry

Our proposed regulator will protect children most effectively if it is able to build productive relationships, and work in collaboration with, civil society, industry and other regulators.

In this section, we set out how the regulatory model ensures meaningful cooperation with, and accountability to, each of these audiences.

Civil society and child protection experts

The regulator should strive to build deep relationships with civil society.

In line with other regulatory examples, the regulator should have a duty to consult with expert groups in the exercise of its functions, including law enforcement and child protection bodies.

We see merit in the establishment of statutory panels, to provide a formal mechanism to consult stakeholders such as the NSPCC and ensure the regulator is able to draw on wider sectoral expertise in the discharge of its functions.

For the social media regulator, this would likely translate into a child protection panel (comprising persons or organisations with a child protection remit or expertise, including charities, law enforcement, and relevant government officials). A separate industry panel should also be established.

There is merit in the adoption of supercomplaint powers, in line with the provisions available to consumer advocacy bodies.[45] These powers would allow designated bodies to raise a complaint about a feature, or combination of features, which appear to be placing children at significant risk of harm. Such a complaint may suggest that a platform is breaching its statutory duty of care.

Relationship with other regulators

In addition to a social media regulator, there are both UK and EU initiatives which may place additional regulatory requirements on platforms. In the UK, the Information Commissioner has recently consulted on its statutory Age-Appropriate Design Code, which will introduce minimum design standards for social networks that offer services to children.

Separately, the EU has been developing a new Audio Visual Media Services Directive, which will likely place new regulatory requirements on video sharing sites, livestreaming sites, and parts of social networks where video content is the primary design feature.[46]

While the scope and extent of wider regulatory requirements is still to be finalised, the relevant regulators should manage any regulatory overlap by establishing a memorandum of understanding between them.

There should also be close regulatory co-operation and knowledge sharing, including processes for the effective transfer of market intelligence, and participation in the UK Regulators Network.

45 Section 11(1) of the Enterprise Act 2002 provides for designated bodies, including Which?, Citizens Advice and sector-specific statutory bodies, to raise a supercomplaint about 'any feature, or combination of features, of a market in the UK for good and services that is or appears to be significantly harming the interests of consumers.'

46 EU member states will have two years to implement the directive into legislation. Transposition into UK law is therefore contingent on whether the UK agrees an implementation period with the European Union for its exit from the European Union, and the timescales for this.

Engagement with industry

Although much of industry is resisting regulation, we consider that an intelligently designed and bounded regulatory model may offer benefits to social media providers.

Regulatory certainty:[47] Some platforms have already recognised that it might be desirable for Government to introduce legal or regulatory frameworks, including in areas that present significant reputational risks.[48]

Clear and consistent regulatory requirements: Our proposed regulatory model would apply to all social media providers, regardless of size and scope. This would ensure platforms have a consistent understanding of their safeguarding responsibilities, and would address the reputational burden in which more responsible platforms are unreasonably maligned by the (in) action of poorer performing unregulated sites.

Removal of commercial barriers to transparency: some platforms may be reluctant to take steps to become more transparent about the scale and extent of risks on their sites, for fear of negative publicity associated with being the first ones to do so. By creating a more level playing field, such disincentives are removed.

The opportunity to build consumer trust: 83 per cent of the public consider regulation to be beneficial for both businesses and consumers.[49] Given the scale and extent of online harms, social networks should embrace regulation as a means of improving their reputational standing.

In developing our regulatory model, we have sought to ensure the regulation should not be too complex, expensive or burdensome.

Our risk-based approach to implementation should enable platforms to focus on substantive compliance, and direct their resources towards tackling the most prominent harms on their sites. This means that they should not have to expend resource on unnecessary technical or procedural measures, or on ensuring compliance against areas where no real harm is taking place.[50]

The model is designed to secure necessary regulatory protections and to minimise any potential barriers to market entry. While we are confident that the regulatory design will not deter innovation, we would encourage the regulator to explore ways to incentivise adoption of best practice, and to support start-ups through the provision of active safeguarding and compliance advice.

Such measures could usefully include:

- providing training to start-ups and new market entrants on how to achieve regulatory compliance, and to do so in a way that is not overly burdensome;
- developing safeguarding guidance for start-ups, including exploring options to facilitate knowledge transfer from existing sites;
- facilitating access for start-ups to 'off the shelf' technical solutions e.g. artificial intelligence tools to proactively detect grooming; and
- creating an innovation hub, similar to the FCA's 'sandbox' model, to enable new market entrants to test innovative products in a controlled environment. This would enable firms to develop new products with regulatory supervision, and to identify necessary design safeguards at the build stage, rather than having to retrofit them.

47 Regulatory certainty is highly valued among regulated bodies. For example, PA Consulting found that 93 per cent of businesses said regulators could support innovation by creating a stronger sense of predictability and certainty for their sector. PA Consulting (2018) Re-thinking Regulators. From watchdogs of industry to champions of the public.

48 Karim Palant, Facebook's UK Policy Manager told the Science and Technology Committee: 'there may be areas where Government may take the view they can provide coordination or a set of rules and frameworks [...] there are areas, absolutely, where we would say that could be a positive.' Q464/465. Oral evidence given on 16/10/18 to the 'Impact of social media and screen use on young people's health' inquiry.

49 ibid.

50 Sparrow, M (2011) The Regulatory Craft: Controlling risks, solving problems, and managing compliance. Washington DC: Brookings Institute.

9. Other considerations

Funding

The regulator should be funded through a levy imposed on social media providers. This is in line with the existing models used for regulatory and consumer advocacy functions, including in the financial services and utility sectors. Careful consideration should be given to the appropriate calculation of costs between platforms, although we would expect the largest platforms should contribute the highest proportion of costs.

Parliamentary accountability

The regulator should be accountable to Parliament when discharging its statutory and regulatory functions and should be required to lay an annual report of its activities before Parliament.

Given the high anticipated interest in the regulator's work, it seems likely that a number of Select Committees would scrutinise its activity, for example the Digital, Culture Media and Sport, Home Affairs, and Science and Technology Select Committees.

Research, public information and advocacy functions

Consideration should be given to the regulator being afforded statutory duties to conduct research into social media use and online harms. Existing regulators already have similar duties, for example Ofcom has a statutory duty to undertake media literacy research.[51]

Consideration should be given to using the funding levy to support separate advocacy, public information and education initiatives.

Regulatory competence

Given the scale and extent of online harms, it is desirable for statutory regulation to be introduced as quickly as possible.

This could take the form of a new regulator, although this would likely require a lengthy set-up period and even longer timings before it is able to deliver impacts that are proportionate to the powers and resources available to it. This would also introduce additional cost and complexity.

An alternative approach is to extend the competence of an existing regulator, most likely Ofcom. Ofcom possesses well-established technical, sectoral and regulatory expertise, and it commands broad respect among industry and civil society.

In recent years, Ofcom has assumed regulatory responsibility for a number of additional functions, including video on demand, postal communications, and regulatory oversight of the BBC. It is therefore well placed to assume this additional area of regulatory competence.

Wider social media harms

Our proposal is for a regulatory model that focuses on, and is designed specifically to tackle, the range of online harms faced by children, in particular to ensure children are protected from technology-facilitated abuse.

While broader harms are outside of the scope of this proposal, we believe the 'duty of care' model represents a readily adaptable regulatory framework that could be applied against other harms, should the UK Government wish to explore a broader approach.

51 Section 14(6a) of the Communications Act 2003.

NSPCC

Everyone who comes into contact with children and young people has a responsibility to keep them safe. At the NSPCC, we help individuals and organisations to do this.

We provide a range of online and face-to-face training courses. We keep you up-to-date with the latest child protection policy, practice and research and help you to understand and respond to your safeguarding challenges. And we share our knowledge of what works to help you deliver services for children and families.

It means together we can help children who've been abused to rebuild their lives. Together we can protect children at risk. And, together, we can find the best ways of preventing child abuse from ever happening.

But it's only with your support, working together, that we can be there to make children safer right across the UK.

nspcc.org.uk

EVERY CHILDHOOD IS WORTH FIGHTING FOR