NSPCC

Delivering a Duty of Care

An assessment of the Government's proposals against the NSPCC's six tests for the Online Safety Bill

March 2021

EVERY CHILDHOOD IS WORTH FIGHTING FOR

Contents

Summary

In December 2020, the UK Government published its final legislative proposals to protect children from online abuse.[1] Legislation could not be more important: the Online Safety Bill is an urgent child protection measure, and it will become a crucial part of the child protection landscape for decades to come.

If it acts with urgency and ambition, the Government can secure an Online Harms Bill that delivers tough but proportionate regulation, and that sets a global standard.

But if the measures fall short, children will continue to face avoidable harm. One in five UK internet users[2] will face online abuse that continues to increase in both scale and complexity, including online sexual abuse. The cost of industry action will continue to be felt by children, families and society.[3]

The NSPCC has led the campaign for a social media regulator – with companies subject to a legally enforceable Duty of Care that requires them to identify reasonably foreseeable risks, and address them through systemic changes to how their services are designed and run.

In conjunction with Herbert Smith Freehills, in spring 2019 the NSPCC published comprehensive proposals for a regulatory model.[4] Last September, we set out six tests that the Online Safety Bill must meet if it is to deliver for children,[5] and to deliver on the Government's ambition to make Britain the safest place in the world to be online.[6]

The NSPCC will judge the Online Safety Bill against each of these tests. Following the December 2020 publication of the Government's final response to the Online Harms White Paper, this report sets out our current assessment of whether the tests are being met. In our scorecard (appendix one), we find that while the Government's response sets out a broadly workable and robust regulatory model, there are a number of significant weaknesses which need to be addressed.

Against each of the six tests, we set out a series of indicators that will determine whether regulation goes far enough to protect children from avoidable abuse.

In nine out of 27 indicators, we find the Government has met our tests (or we are broadly satisfied with the proposed approach.) However, in a further nine indicators, our tests have been largely or wholly unmet.

To fully deliver for children, the Government should adopt a more ambitious and child-centred approach in some key areas of the Bill. In particular, it must:

Ensure regulation addresses the cross-platform nature of risks: well-established grooming pathways see abusers exploit the design features of social networks to make contact with children, before they move communication across to encrypted messaging and livestreaming sites.[7] Similarly, harmful content spreads with considerable velocity and virality across social networks and messaging sites.

Ofcom must therefore have a legal duty to address the cross-platform nature of risks, with clear expectations on companies that meeting the Duty of Care means having processes in place to share data on offending behaviour, and on highly agile and constantly evolving threats;

Take a clearer and more robust approach to activity that facilitates illegal behaviour, but which may not meet the criminal threshold. Unless the Online Safety Bill gives the regulator powers to treat content that facilitates child abuse with the same severity as illegal material, legislation will fail to tackle egregious material upstream. Abusers will still be able to organise in plain sight, post 'digital breadcrumbs' that signpost to illegal content, and re-victimise children through the sharing and viewing of carefully edited child abuse sequences;

Strengthen its proposed enforcement regime, through introducing senior management liability that is directly linked to the discharge of the Duty of Care. The Government has significantly weakened its ambition: under its proposals, senior managers will no longer be held personally accountable for decisions on product safety, only for narrow procedural failings; and even then not until at least two years after regulation takes effect.

[1] UK Government (2020) Final Response to the Online Harms White Paper
[2] Data from the Information Commissioner's Office
[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 sheets of companies, but of society'
[4] NSPCC (2019) Taming the Wild West Web: How to regulate social networks and keep children safe from abuse
[5] NSPCC (2020) How to win the Wild West Web: Six tests for delivering the Online Harms Bill. London: NSPCC
[6] UK Government (2019) Online Harms White Paper
[7] Europol (2020) Internet organised crime threat assessment. Lyon: Europol

There is a substantive risk this enforcement approach will not adequately incentivise compliance, and fail to deliver the extent of cultural change that is required. Unless the Government strengthens its position, with a senior management scheme that focuses minds on whether online services are safe, and supported by the option of criminal and financial sanctions in respect of the most serious breaches, this will fail to offer necessary deterrence value. In our assessment, effective enforcement powers may significantly undermine the regulator's effectiveness, and;

Deliver a bolder and more ambitious approach to user advocacy: As part of the online harms arrangements, the Government must commit to a dedicated user advocacy voice for children, funded by the industry levy. This is essential to create a level playing field for children – to ensure there is an effective counterbalance to industry interventions, and provide the regulator with credible and authoritative evidence, support and challenge. The Government should draw more directly on what exists in other regulated sectors, from postal services to transport, where the user voice is funded and empowered. Children are potentially the most vulnerable of all users – and they deserve a regulatory settlement that affords the strongest possible protections from abuse.

As we demonstrate, there are some clear areas where our tests are either partially or substantially unmet. The Government now has the chance to fix this before it publishes a draft Bill.

If regulation is poorly designed, or the regulator isn't equipped with the powers and tools it needs, children will continue to face otherwise preventable harm.

But if these issues are addressed, the result will be a highly effective regulatory regime, and a Duty of Care that gives children online protections that are long overdue.

Our six tests for the Online Safety Bill

1. Regulation must have, at its heart, an expansive **principles-based duty of care**, capable of driving cultural change;
2. Regulation must meaningfully **tackle child sexual abuse;**
3. The Duty of Care must meaningfully address **legal but harmful content,** both content and how it is recommended to users;
4. There should be **effective transparency requirements and investigation powers** for the regulator, with information disclosure duties on regulated firms;
5. We need to see an **enforcement regime capable of incentivising cultural change**, which should include senior management liability, and criminal and financial sanctions; and
6. There needs to be **user advocacy** arrangements for children, including a dedicated user advocate voice, funded by the industry levy, so children have a powerful voice in regulatory debates.

Test one: The Duty of Care

The Online Safety Bill must set out a well-designed, proportionate regulatory framework that can deliver the strongest possible protections for children. That means the adoption of a principles-based approach, underpinned by a broad and future proofed Duty of Care.

Against this test, we are broadly pleased with the Government's approach. In our scorecard, our measures have either been met (or in a number of cases will be determined by Ofcom's regulatory scheme.)

Systemic Duty of Care

We strongly welcome the Government's commitment to a Duty of Care, with a requirement on platforms to identify and act on content or activity which presents a reasonably foreseeable risk of significant adverse physical or psychological harm to children. Companies will be required to understand the risks to individuals using their services, including those that result from their design and operation, and must put in place appropriate systems and processes to improve safety and to monitor their effectiveness.

This systemic approach is desirable precisely because it requires platforms to demonstrate the potential risks to children have been actively considered when making decisions, and their products are consequently safe by design. The Duty of Care model means that online services cannot demonstrate compliance solely in terms of attendance to a prescriptive set of requirements.

It reflects the model outlined by the NSPCC's regulatory proposal, and the original Duty of Care approach set out by Perrin and Woods.[8]

Broad regulatory scope and definition of harm

The regulatory regime will be broad in scope, encompassing online services that host user generated content and/or that facilitate public or private user interactions. The Duty of Care applies to search engines, consumer cloud storage services and gaming products that enable user interaction. It doesn't apply to app stores.

All online services in scope will be required to tackle illegal content, and if likely to be accessed by children, will also be required to take action to prevent exposure to legal but harmful content.

If an online service is likely to be accessed by children, the site will need to make clear what it considers to be acceptable content, and must provide appropriate risk based, proportionate measures, in line with a code of practice.

The Government intends to specify priority categories of content that is illegal or harmful to children in secondary legislation, building on a broad definition of harm in primary legislation. For each priority issue, platforms will need to consider, based on a risk assessment, what systems and processes are necessary to identify, assess and address the potential for illegal or harmful behaviour.

Platforms likely to be accessed by children will need to undertake regular child safety risk assessments, to identify and implement age appropriate measures that protect children from reasonably foreseeable risks (and to identify new or emerging harms). The regulator should ensure that there are clear incentives for platforms to identify emerging risks, including as a result of introducing new products or technology.

It will be crucial that the regulator sets out the intended frequency, and provides clear parameters about the quality of risk assessments it expects.

Effective Codes of Practice

Ofcom will have a duty to issue statutory codes of practice that set out steps companies can take to fulfil the Duty of Care. Companies may take alternative steps to those set out in the codes, as part of an outcome-based approach, provided they can demonstrate to Ofcom these are as effective or exceed the standards set out in them.

While it is our understanding that codes are designed to be non-exhaustive and to steer, rather than direct, how platforms comply, there remains a risk the codes are either drafted or interpreted in a way that becomes unhelpfully prescriptive.

The Government will set objectives for the codes, and ministers will have the power to reject a draft code and require the regulator to make modifications, for reasons relating to government policy.

[8] Perrin, W and Woods, L (2019) Internet harm reduction: a proposal. Dunfermline: Carnegie UK Trust

Incentivising cultural change

If implemented correctly, the Duty of Care is a purpose driven and highly agile approach – and it should actively hardwire compliance into firms. But it must also deliver a far greater prize: the emphasis on systemic risk should bring about much-needed cultural change across platforms that have previously been able to decide for themselves whether and how they protect children.

This must be a primary objective of the legislation. Although the adoption of a principles based Duty of Care will be a significant enabler for a shift in how online services design and deliver their products for children, it will be vital that both the Government and Ofcom consistently seek to maximise opportunities for cultural change, both in the design of the regulatory scheme and its enforcement mechanisms.

We therefore encourage Government to adopt, as one of the guiding principles for the regulatory framework, a requirement for Ofcom to incentivise this when developing its regulatory scheme. It should report on the effectiveness of these efforts as part of its annual report.

Test two: tackling online child abuse

The regulator must be ambitious and determined in its commitment to tackling online child abuse. Ofcom will be judged in how effectively it can protect children from abuse risks that continue to grow, both in scale and complexity.

In our scorecard, we find that our test has been partially met. In four out of eight measures, the Government's proposals fully or partially meet our expectations. However, in two key areas, including the importance of adopting a cross-platform approach to risk, and adequately tackling content that facilitates child abuse, our tests remain unmet.

The Government's proposals have a clear emphasis on tackling technology facilitated sexual abuse, with all regulated services being required to take action to prevent illegal activity on their sites. The Government will set out priority categories of offences in secondary legislation, which should include both online grooming and the production and distribution of child abuse images. To demonstrate compliance, platforms will need to demonstrate robust systems and processes to detect and disrupt these most harmful of activities.

Ofcom will have a specific duty to consider the vulnerability of children when performing its functions. The regulator's primary duty will be to protect the safety of users of online services, and to ensure a higher level of protection for children than adults.

Much will rest on the scope and ambition of Ofcom's codes of practice, the demonstrable exercise of a risk-based approach[9], and its understanding of the highly agile and constantly evolving nature of online threats against children.

An effective child abuse response

Platforms should be expected to demonstrate to the regulator the consistency and sufficiency of their child abuse response. This should include, but certainly not be limited to, the scope and effectiveness of their takedown processes; measures to proactively detect and disrupt new images being produced; and mechanisms to proactively detect and report online grooming.

The regulator should require platforms to take measures to substantially frustrate the potential for their design features to be readily exploited by abusers. It should also develop its regulatory scheme with a clear understanding that a satisfactory response will need to exceed the action currently undertaken by many sites. Ofcom should avoid a default assumption that the current approaches of the larger firms are the upper limits of what is required.

Ofcom must be prepared to investigate platforms that do not appear to be enforcing their takedown processes appropriately and, as part of its risk based approach, should closely supervise the effectiveness of them. It might usefully signal this will be a priority area for thematic review.

The Canadian Centre for Child Protection, whose Project Arachnid tool has identified 6.1 million images since 2016, has found that some sites routinely refused to comply with takedown requests of children aged as young as 9 or 10.[10] Some platforms argue that if there is any (even very early signs) of sexual maturation, it is not appropriate for them to take down images, unless the age and identity the child is already known.

[9] Reflecting the risk-based model advocated by Sparrow (2011) in which the regulator focuses on those harms that most impede regulatory outcomes. Sparrow, M (2011) The Regulatory Craft. Washington, DC: Brookings Institution

[10] Canadian Centre for Child Protection (2019) How we are failing children: changing the paradigm. Winnipeg: CCCP

For the first time, there will be a legal requirement for online services to report abuse on their sites, with the potential of UK-based arrangements being established to process these reports. However, we expect most reports will continued to be funnelled through the National Center for Missing and Exploited Children (NCMEC), which will continue to act as the 'global clearing house' for child abuse referrals.

Tackling the risks of private messaging

We strongly welcome the Government's decision to significantly broaden the scope of its proposals to include private messaging, and to mitigate the significant adverse impacts of end-to-end encryption (E2E).

Put simply, online harms regulation cannot succeed unless its scope includes the product features and design choices that pose the greatest risks for children.

Recent data from the Office for National Statistics (ONS) shows that private messaging plays a central role in contact between children and people they've not met offline before. When children are contacted online by someone they don't know in person, in nearly three quarters (74%) of cases, this contact initially takes place by private message.[11]

Some 12 million of the 18.4 million worldwide child sexual abuse reports made by Facebook in 2019 related to content shared on private channels.[12]

End-to-end encryption presents very significant risks to children, because it effectively prevents platforms from being able to identify and disrupt child abuse on their services. In turn, this significantly reduces referrals to law-enforcement, and it impedes their ability to investigate offences.[13] The National Center for Missing and Exploited Children estimates that 70% of Facebook's reports could be lost if the proceeds with E2E before appropriate mitigations are in place.[14]

In recent evidence to the Home Affairs Select Committee, Facebook acknowledged that the introduction of E2E would lead to a fall in the number of child abuse reports they generate, but insisted they would push ahead anyway. In doing so, they cited an intention to meet an apparent 'industry standard.'[15]

Under the government's proposals, the regulator would be able to compel platforms to use automated technology to detect online child abuse content or activity (where alternative measures cannot be deployed or have not been successful.)

The use of these powers will be subject to a stringent set of safeguards, with the regulator required to publish an annual report on the effectiveness and accuracy of automated tools it might wish to employ, and having to seek ministerial approval before it issued an enforcement notice.

While we support the principle of such powers being deployed in a proportionate way, with appropriate safeguards in place, we are concerned that the proposed process sets a very high bar before regulatory action could occur. In practice, it might be highly challenging for the regulator to exercise these powers.

This is because:

- The regulator will need to demonstrate there is 'persistent and prevalent child abuse' before it can instruct a platform to take additional measures. However, there are significant questions about how such a high evidential threshold can be met, when end-to-end encryption is likely to result in a steep fall in reporting volumes;
- Ofcom would need to be satisfied that a platform has failed to address such persistent and prevalent abuse, but companies might be able to offset this risk by reporting superficially high metrics that might be suggestive of a highly effective response, but cannot easily or readily be understood in the context of overall volumes of abuse;[16]
- The regulator will need to be satisfied that no alternative, less intrusive approaches are available. It is unclear what happens if such remedies may be technically possible, for example through on-device hash scanning, but are only technically possible with the cooperation of third-party is that outside of regulatory purview.

It would be beneficial for the regulator to be able to take enforcement action at an earlier stage, where a platform is unable to demonstrate that high-risk design features can meet the Duty of Care. This assessment should be informed by a risk assessment from the platform that sets out the likely impact of a high-risk design feature on the ability to detect child abuse.

Ofcom should also consider the interplay of end-to-end

[11] Office for National Statistics (2021) Children's online behaviour in England and Wales: year ending 2020. Newport: ONS

[12] NCMEC figures

[13] Europol suggest end-to-end encryption poses a 'substantial risk' in terms of online child abuse. Europol (2020) Internet organised crime threat assessment. The Hague: Europol

[14] In 2020, Facebook made 20.3 million reports, which could mean over 14 million reports being lost

[15] Remarks made by Monika Bickert, Facebook's vice-president of global policy management, in evidence to the Home Affairs Select Committee on January 20th 2021

[16] Disclosure reporting often tends to emphasise the publication of metrics, but without contextualised information that allows an assessment of the resulting impact and scale of platform response. Douek, E. (2020) The rise of content cartels: Using transparency and accountability in industry-wide content removal decisions. New York City: Knight First Amendment Institute, Columbia University

encryption with other design features. The potential for risk is likely to be exacerbated if there is significant operational relationship with other high-risk design choices, for example WhatsApp's proposals to auto-delete all messages by default.[17] Europol has cited this design feature as being particularly problematic for child abuse detection.[18]

Similarly, the regulator should assess whether an online service seeks to bundle multiple design features under a single end-to-end encrypted cloak. If multiple parts of the user journey are end-to-end encrypted, groomers could potentially message a child and then coerce them into producing self-generated videos on video chats, with the platform being unable to identify or disrupt abuse at any stage of the grooming process.

In this respect, Facebook's proposal to end-to-end encrypt both private messages and its Messenger Rooms videochat product, on a platform which also allows algorithmic recommendation of users, represents a hugely problematic product offering.[19]

In recent weeks, Twitter's CEO Jack Dorsey has reiterated his support for decentralised social networks, in which platforms may effectively engineer away their ability to perform content moderation altogether.[20]

If it is neither possible to effectively mitigate risks through technology, nor for the regulator to act until there is significant and demonstrable harm already occurring, it is conceivable the regulator might have to consider service blocking – or it might reach a regulatory dead-end while considerable harm continues to occur.

Embedding a cross-platform approach to risk

The proposed regulatory framework fails to adequately reflect the cross-platform nature of many online risks to children.

While platforms will be responsible for harms to individuals that happen as a direct consequence of the design of their site, or activity enabled by it, we have significant concerns that the regulatory expectations on firms won't address the ways harms typically extend or proliferate across multiple services.

Online abuse is rarely siloed on a single platform or app. For example, we see well established online grooming pathways, in which abusers exploit the design features of social networks to make effortless contact with children, before the process of coercion and control over them is migrated elsewhere. Harmful behaviour can spread at considerable velocity across social networks and video sharing sites.[21] An abuser may be playing video games with a child while grooming them on ancillary chat platform, such as Discord.[22]

If the regulatory regime is to be effective, it must require a systemic response to cross-platform risks. Platforms have already demonstrated this is achievable through, for example, the rapid response arrangements established after the Christchurch attack. TikTok has called for an industry-wide scheme to identify and takedown harmful content, aimed at preventing the speed with which content can proliferate.[23]

It is therefore vital that there is a statutory duty on Ofcom to consider the cross-platform nature of risks when discharging its functions.

In turn, Ofcom's codes of practice should place specific obligations on platforms to share threat assessments, develop mechanisms to share offender intelligence, and ensure a more coherent systemic approach to addressing an online ecosystem in which unmitigated harms might otherwise be allowed to flourish.

Addressing content that facilitates illegal behaviour

The Government's final White Paper response fails to adequately address the growing challenge of content that facilitates illegal behaviour, but that may not in and of itself meet the criminal threshold for removal.

Many firms have been reluctant to shift from a clear but arguably reductionist consensus on the definition and dimensions of the child abuse problem. For the purposes of content moderation, many platforms have adopted an approach where they focus on illegal child abuse material, because it is seen by them to 'clearly and objectively meet a concrete definition.'[24]

[17] Mark Zuckerberg's comments to an all-staff meeting in January 2021 were reported by the Daily Telegraph and Buzzfeed News

[18] Europol (2020) Internet organised crime threat assessment. The Hague: Europol

[19] Facebook Rooms allows up to 50 participants to join a call, who do not need to have Facebook accounts to join

[20] In a tweet thread on 14th January, Jack Dorsey set out Twitter's plans for a decentralised social media model with a goal for it to be the 'standard for the public conversation layer of the internet [...' that is not controlled or influenced by any single individual or entity.'

[21] For example, in September 2020 a graphic video of a suicide, first livestreamed on Facebook, spread rapidly on platforms including TikTok and YouTube. Gilbert, D (2020) Facebook refused to take down a livestreamed suicide, now it's all over TikTok. Published by Vice News

[22] Helm, B (2020) Sex, lies and video games: Inside Roblox's war on porn. Published in Fast Company magazine.

[23] TikTok (2020) TikTok proposes global coalition to protect against harmful content, blogpost on TikTok;s website

[24] According to Evelyn Douek, who notes there is a consensus among industry that the 'desirability and definition of child sexual abuse material is quite properly well settled' and that continual re-evaluation of the child abuse threat is not necessary. However, the definitional parameters are far from settled – for example, the Budapest Convention defines fabricated images as illegal, but the US legal parameters do not, an issue which is likely to become more pressing with technological change. Douek, E. (2020) The rise of content cartels: Using transparency and accountability in industry-wide content removal decisions. New York City: Knight First Amendment Institute, Columbia University

There is a compelling case this approach does not go far enough, and that platforms should be required to identify and act on images that may not meet the current criminal threshold, but which can facilitate access to illegal images; act as 'digital breadcrumbs' that allow abusers to identify and form networks with each other; and to actively revictimise children through the sharing and viewing of carefully edited abuse sequences.

In particular, the regulator must be prepared to tackle so-called 'abuse image series'. In many cases, abusers will upload or seek to access material containing large numbers of images taken in the run-up to or following sexual abuse, effectively forming part of a sequence that culminates with images or videos that meet the criminal threshold. In some cases, these are deliberately used by abusers because they anticipate such images won't be proactively removed by the host site.[25]

Given the clearly egregious nature of such material, and its direct contribution to driving illegal activity, the Government must act. The Online Safety Bill should grant the regulator powers to treat content that facilitates child abuse with the same severity as illegal material, with clear expectations on firms to adopt a more proactive and child centred approach to takedown.

This is a proportionate and highly targeted approach, and cannot reasonably be opposed on freedom of expression grounds. It is entirely consistent with the clear, upstream approach advocated by the Duty of Care.

Test three: tackling legal but harmful content

If regulation is to succeed, it must tackle clearly inappropriate and potentially harmful content. This includes material that promotes or glorifies self-harm and suicide, which most major sites prohibit but often fail to moderate effectively. In many cases, the potential for harm is likely to come from platform mechanisms that promote or algorithmically recommend harmful content to users.

Our scorecard raises concerns about the Government's proposed approach, with much resting on how Ofcom develops its regulatory scheme, and whether its codes of practice adopt a suitably child-centred and harm based approach.

The most serious legal harms continue to affect children at scale, and underline why action to protect children is so essential. Facebook's own figures suggest that up to 5 in every 10,000 views contain prohibited material that glorifies and promotes self-harm and suicide.[26] This is likely to be a significant under estimate for vulnerable children being served up such content through algorithmic profiling.

The Government's proposals

Under the Government's proposals, all online services likely to be accessed by children will have to take reasonable and proportionate measures to prevent them being exposed to harmful content. The Government will set out a list of priority legal but harmful risks in secondary legislation.

Platforms likely to be accessed by children will have to clearly specify what content is deemed acceptable in their terms and conditions. Companies will be required to conduct regular child safety risk assessments, identify and implement proportionate mitigations to protect against reasonably foreseen risks, and have processes in place to monitor their effectiveness.

Although the Government has somewhat strengthened its proposals for legal but harmful content, a number of concerns remain, as set out below.

Avoiding differential protections

While all platforms likely to be accessed by children will have to protect children from harmful and age inappropriate content, only the largest and highest risk online services (designated as category one providers) will have to take similar measures to protect adults. This means that the effectiveness of age assurance measures become particularly important on smaller sites (category two providers), even though smaller sites are by definition less likely to have a more developed age assurance response.

There is also a risk that smaller sites may increasingly become vectors of harmful and inappropriate content, if regulatory requirements place differing expectations on them. This is likely to prove particularly problematic if the government does not agree to adopt a strengthened approach to content that facilities illegal behaviour, including child abuse.

[25] Canadian Centre for Child Protection (2019) How we are failing children: changing the paradigm. Winnipeg: CCCP
[26] Transparency reports available on Facebook's website

To address the risk that platforms could face a perverse incentive to adopt weaker community standards, in order to face less onerous regulatory requirements, sites will now need to demonstrate compliance against a Code of Practice that sets out appropriate levels of risk based, proportionate action for each of the priority measures. However, there is likely to be significant contention about which legal harms will be included in secondary legislation, and the scope and extent of expectations to be placed on category one providers.

As a result, there is likely to be a concerted push by larger providers where they lobby the regulator in respect of both its guidance to Government and the development of its Code of Practice. This may come as part of a coordinated strategy to downplay the perceived impact of some harms (and to emphasise the potential for unintended consequences from more onerous requirements), including the commissioning of third-party actors and funded research to make this case.[27] Ofcom will need to be mindful of the skewing potential this could have on the development of its regulatory scheme.

Any differential application of the Duty of Care would fail to offer children the protection they need if it poorly reflects, or is unable to adequately respond to, the full extent of online harms to which they are likely to be exposed.

Legislation must recognise that the potential for harm cannot be understood solely in terms of the legality of online content or behaviour. A 'two track' approach must not result in children receiving diminished protection.

Capturing commercial pornography sites

Following the Government's decision not to proceed with part three of the Digital Economy Act, which made provision for age verification for commercial pornography sites, measures to restrict access to pornography will now be taken forward as part of the Online Safety Bill.

While this presents some advantages, including the requirement to prevent exposure to age inappropriate content being extended to all social media sites, it appears the proposed scope of the legislation has erroneously excluded many commercial pornography sites (those that do not host user generated content or allow user communication).

The Government should amend the scope of their proposals, prior to publishing a draft Bill, to explicitly capture all commercial pornography sites.

Test four: transparency and investigation powers

Although the Government proposes to give the regulator a strong set of transparency and information disclosure powers, we are concerned that the lack of information disclosure duties risks failing to actively hardwire the Duty of Care into corporate decision making. The proposals fail to adequately adopt effective regulatory design from other sectors. The result could be that Ofcom is less equipped than other regulators to understand a fast moving and highly agile sector, and correspondingly, the risks that may result.

Transparency and information disclosure is crucial to the regulator's work, and is arguably as important as enforcement powers that inevitably tend to attract more attention. A close relationship between regulator and platform is essential, which includes transparency and scrutiny on the regulator's terms.[28]

Our scorecard finds that this test is only partially met, with two of five indicators relating to disclosure duties not met at all.

Transparency and investigatory powers

Comprehensive transparency powers are crucial to the regulator's success. Unless Ofcom has robust investigatory and information disclosure powers, there will be a clear information asymmetry between them and tech firms, and this could mean the regulator is forced to take decisions on low quality evidence or is less inclined to propose more ambitious measures.[29]

It appears Ofcom will be given reasonably substantive investigatory powers, most likely through the extension of its existing powers under sections 135-146 of the Communications Act. The Government's response

[27] Abdalla, M et al (2021) The Grey hoodie project: Big Tobacco, Big Tech and the threat to academic integrity. Pre-print. Cambridge, MA: Harvard.

[28] Beverton-Palmer, M et al (2020) Online harms: bring in the auditors. London: Tony Blair Institute for Global Change

[29] Loutrel, B (2019) Creating a French framework to make social media platforms more accountable: acting in France with a European vision. Paris: French Government

commits to granting Ofcom broad powers to require companies to provide the information that the regulator needs to carry out its functions. Crucially, this will apply to both online services in scope of the Duty of Care, and where necessary, to other organisations that may have relevant information, for example app stores or third parties that support platforms to discharge their regulatory duties.

The Government will grant the regulator investigatory powers that have worked well in financial services regulation, including the ability to commission a Skilled Person report where it has concerns about a platform or it requires further understanding of the adequacy of its processes. Ofcom will have powers to commission a review, and when necessary appoint the 'skilled person' to conduct it, with the regulated party being liable for the costs involved.

The regulator will also be able to interview staff to assist its investigations, which will offer particular benefit if coupled to a more effective senior management liability scheme.

Effective transparency reporting

The Government will proceed with annual transparency reports, but only for large and higher risk category one sites. Such arrangements will only be beneficial if they provide significant and interrogable information, compared to existing approaches that have been widely dismissed as a form of 'transparency theatre.'[30]

There are understandable trade-offs involved in the level of transparency that should be expected, for example the risk that data enables bad actors to gain the system. However, it will be important that the regulator takes an ambitious approach to transparency requirements, with decisions on disclosures ultimately being driven by the public interest, not that of the companies.[31]

The Government should consider proposals for transparency reports to be either externally audited or subject to quality assurance activity led by the regulator. This will build confidence in the quality and robustness of regulatory disclosures, and minimise the risk that platforms seek to present data in a selective or potentially inaccurate way. The German authorities have issued fines to Facebook for under-reporting against the transparency arrangements in that country's hate speech regulation.[32]

Facebook's most recent corporate voluntary transparency report underlines why effective regulatory scrutiny is needed: in the most recent quarter, child abuse reports dropped by more than half, to 5.4 million, on its Facebook platform, citing problems with its technology; and by 20 per cent on Instagram, which cited renewed issues with human moderation capacity during lockdowns.[33] This report raises as many questions as it provides answers – for example, why it appears Facebook's products have differing levels of resilience during the pandemic.

Proactive information disclosure duties

We are disappointed the Government have not placed broad but workable information disclosure duties on platforms.

Category one services should face regulatory duties to proactively disclose information to the regulator about which it could reasonably expect to be informed about. For example, companies should notify Ofcom about significant changes to their products or services, or to their moderation arrangements, which may impact upon the child abuse threat and its response to it.

A similar proactive duty[34] already applies in the financial services sector. Although potentially broad, the scope of this duty can be drawn with sufficient clarity that social media firms can properly understand their requirements, and that companies do not face unmanageable reporting burdens.

Such companies should also be subject to 'red flag' disclosure requirements, in which they would be required to notify the regulator of any significant lapses in or changes to systems and processes that compromise children's safety or could put them at risk.[35] For example, if regulation had been in place over the last 12 months, Facebook might reasonably have been expected to report on the technology and staffing issues which it attributes to its reduced detection of child abuse content.

Experience from the financial services sector demonstrates the importance of disclosure duties to act as an important means of regulatory intelligence gathering; but perhaps more importantly, to provide a useful means of hardwiring regulatory compliance into company decisions on the design and operation of their sites.

[30] Douek, E. (2020) The rise of content cartels: Using transparency and accountability in industry-wide content removal decisions. New York City: Knight First Amendment Institute, Columbia University

[31] Current transparency reporting tends to emphasise the publication of metrics, but without contextualised information that allows an assessment of the resulting impact and scale of platform response. See Evelyn Douek's analysis of hashing metrics in the GIFCT transparency reports. ibid

[32] Reuters (2019) Germany fines Facebook for under-reporting complaints. Published July 2nd 2019.

[33] Facebook transparency report, available on Facebook's website

[34] Principle 11 of the financial services regime

[35] Again, similar measures are used effectively in other regulated contexts. 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

Test five: enforcement powers

If online harms regulation is to succeed, the regulator must have suitably broad enforcement powers and be able to hold non-compliant sites to account.

This reflects the principle that the platforms that create risks should be responsible for the costs of addressing them. For too long children, families and society have been left to bear the devastating emotional, mental and physical (as well as social and economic) costs of child sexual abuse.

We have significant concerns that the proposed enforcement approach set out in the Government's final white paper response does not go far enough to incentivise compliance. In our scorecard, two of our four measures remain unmet.

Effective financial penalties

We welcome that the Government has proposed much steeper financial penalties than originally envisaged for companies that breach their regulatory obligations. Companies will now face fines of £18 million or ten per cent of turnover (whichever is higher.) Fines of such magnitude will clearly only be levied in respect of the most serious regulatory failings.

However, for the largest companies, the deterrence value of such fines remains unclear. The largest tech companies have billions sitting in the bank as 'cash in hand', and making no returns for shareholders. In this context, the micro economic effects of fines will be blunted, and are likely to have limited impact at best on the marginal behaviours of either the management team or shareholders.

In any event, investigations and appeals can be lengthy, and by the time proceedings are concluded business models may have shifted, with fines and legal proceedings simply "priced in" as a cost of doing business.[36]

Business disruption measures

The government proposes a range of business disruption measures, including the power to make online services withdraw non-compliant products. In the most serious breaches of the Duty of Care, the regulator could seek a court order that would require the likes of ISPs, app stores and cloud hostage services to prevent harmful platforms from being accessible in the UK.

These provisions are much more substantive than those set out in previous legislation, for example the ISP blocking powers proposed in the Digital Economy Act.

Business disruption measures may usefully target smaller or extraterritorial platforms, against which it might otherwise be more difficult to exercise regulatory jurisdiction. However, there is an extremely low possibility this would ever be applied to the largest platforms. Any implementation of the measure against a category one provider would inevitably result in significant and legitimate opposition on the grounds of freedom of expression (and potentially competition and plurality).

Robust senior management liability

Given the serious nature of the harms in scope, and the limitations of the measures set out above, it is clear that the regulator will require additional and more robust enforcement mechanisms to ensure compliance. These must be proportionate to the size and scale of the companies in scope, and capable of incentivising behavioural change in companies that might otherwise continue to put children at risk.

However, the Government's decision to scale back its proposals for named director responsibility raises significant questions about whether the enforcement regime will offer adequate deterrence value to ensure some category one providers step up to their regulatory responsibilities.

Based on the experience of other regulated sectors – principally financial services – there is a compelling case for both corporate and senior manager liability.[37] The Bill should introduce a Senior Managers scheme that imposes personal liability on directors whose actions consistently and significantly put children at risk.

Senior managers exercising a 'significant influence function' would be subject to a set of conduct rules. These would reinforce corporate level requirements on platforms; and crucially, incentivise them to internalise the Duty of Care in their decision-making and the delivery of their functions.

Under such a scheme, the regulator could bring proceedings against senior managers that breach their responsibilities to children, with proportionate sanctions such as fines, disbarment or censure.

For the most significant failings, where initial regulatory proceedings against a senior manager were not appropriate, financial and criminal sanctions could be considered. We envisage criminal sanctions would only ever be considered in extremis, where there was clear evidence of repeated and systemic failings that resulted in a significant risk of harm. Nevertheless, the significant

[36] Centre for Data Ethics and Innovation (2020) Online targeting: final report and recommendations. London: HM Government

[37] Chiu, I (206) Regulatory duties for directors in the financial services sector, and directors duties in company law – Bifurcation and Interfaces. Journal of Business Law, 2016.

deterrence value, and clear potential for adverse reputational effects, are obvious.

In its final response, the Government substantively watered down their plans. Legislation will now include provision for criminal sanctions against directors, but crucially, only in respect of the failure to co-operate with information requests and investigations.

Senior management liability does not apply at all in respect of actual breaches of the Duty of Care – the substantive decisions that managers will take that determine where their products are systemically safe for children to use. It is difficult to see how the clear separation of any form of senior management liability from the actual discharge of the Duty of Care will sufficiently incentivise compliance, nor adequately drive cultural change to the extent that is required.

Under the Government's proposals, even this diluted power would not be introduced until at least two years after the regulator takes effect, following a review of the regulatory framework.

Industry groups have fiercely opposed personal liability. In the final response, the Government notes that companies expressed concerns about 'potential negative impacts on the attractiveness of the U.K. tech sector.'[38] As it stands, the Government's proposals are now weaker in this regard than the draft Online Harms legislation recently published in Ireland, which includes criminal sanctions for both regulatory breaches and a failure to cooperate with investigations.[39] Clearly, tech firms are significantly more important to the economy in Ireland relative to the UK.[40]

If the enforcement mechanisms are not bolstered, the Government risks failing to learn the lessons of effective regulation in other sectors – and it might deliver a regulatory regime that cannot adequately incentivise compliance. Given the clear potential for this to substantially compromise the impact of the other measures in the Bill, we urge the Government to reassess its position.

Test six: user advocacy arrangements

Under the Government's proposals, Ofcom will have a duty to establish ongoing mechanisms for user advocacy. The regulator will need to demonstrate it is capable of understanding the experience of service users, including children. However, the Government needs to be much more ambitious in its plans.

Our scorecard underlines the need for further action, with two out of three measures currently unmet.

Creating a strong advocate for children

The Online Safety Bill must make provision for a statutory user advocacy voice for children, funded by an industry levy. Statutory user advocacy is vital to ensure there is an effective counterbalance to well-resourced industry interventions; and to ensure civil society can offer credible and authoritative support and challenge.

The regulator is unlikely to deliver the best possible outcomes for children unless there is a strong, authoritative and resourced voice that can speak for children in regulatory debates; can support the regulator to understand often complex child abuse issues; and demonstrate emerging areas of concern at an early stage, with the resources and expertise necessary to develop high-quality evidence of a sufficient regulatory threshold.

At present, a range of civil society organisations represent children. However, it should not be taken for granted that civil society and charitable organisations can continue to perform these activities in perpetuity, or to the level and extent that is necessary to support, and where necessary to offer challenge, to the regulator.

If there is an inappropriately scaled, poorly focused or insufficiently resourced civil society response, this is likely to significantly weaken the regulator's ability and appetite to deliver meaningful outcomes for children.

This is also particularly important given the heavily limited potential for children to exercise the redress options that the Government proposes for adult users.[41]

Tech firms are a well-resourced and powerful voice, and will inevitably seek to exert strong influence when decisions are made about their services. It is highly likely

[38] HM Government (2020) Final response to the Online Harms White Paper. London: HM Government

[39] The General Legislative Scheme published by the Irish Government in December 2019

[40] Facebook's own data suggests it added 648 million euro to Irish GDP between 2011 and 2018. IHS Markit: The economic contribution of Facebook data centres in Denmark, Ireland and Sweden (2019) Available on Facebook's website. Digitally-intensive sectors were estimated to be worth 44 billion euro to the Irish economy by 2020, and in 2017, accounted for10.6 per cent of all employment. Data from Technology Ireland (2017) Brexit and the Irish technology sector. Dublin: Technology Ireland.

[41] There is a significant cognitive burden associated with user empowerment on online services, which will likely be heightened for children and young people. Centre for Data Ethics and Innovation (2020) Online targeting: final report and recommendations. London: HM Government

that some companies may seek to frustrate or delay the regulator's work and prevent Ofcom from building a full understanding of the impact of their services on children.

Powerful industry interests are not unique to the tech sector, but the size of and resources available to category one companies are arguably distinct. In the development of online harms regulation, there is a balancing act between allowing the proposed regulatory duties to promote innovation,[42] and ensuring children – perhaps the most vulnerable of all user groups – are protected.

In most other regulated markets, these risks are addressed through strong, independent advocacy models.[43] Without such arrangements in place for online harms, there is a clear risk the children's interests will be asymmetrical to those of industry, and unable to compete effectively with their worldview.

Ofcom is the right regulator for online harms, but its remit to protect service users is not an easy one – and it will be particularly challenging when it comes to children. At present, the Government's emphasis is on user representation: it proposes expert panels, user groups or focus groups.

But if the regulator is to truly adopt a child centred approach, and arrive at child centred outcomes in its decision-making, these mechanisms seem wholly insufficient when compared to strong user advocacy arrangements in other regulated sectors.

Creating a level playing field for children means drawing more directly on what exists in other regulated settlements , from postal services to public transport, where the user voice is funded and empowered. Children are potentially the most vulnerable of all users and they deserve the strongest possible set of protections.

The industry levy is an appropriate mechanism for funding such user advocacy arrangements: this is entirely consistent with the well-established 'polluter pays' principle, and it is a wholly proportionate and reasonable set of costs when considered in terms of the commercial return available to platforms that offer their services to children, but fail to adequately protect them.

Effective supercomplaints process

We support the Government's proposals for supercomplaints, where there is substantial evidence of a systemic issue affecting large numbers of people or specific groups. Supercomplaints will need to focus on the systems and processes that companies have in place, and will usually need to focus on issues occurring across multiple platforms.

The supercomplaints scheme will need to be carefully designed: Ofcom rightly intends to set a high evidentiary threshold for complaints, which is important to avoid it being flooded with a large number of complaints, and to deter poor quality and speculative submissions.

However, the regulator will also need to be mindful of the barriers that civil society organisations may face when seeking to build a supercomplaint case. These include financial constraints; and the self-evident challenge in being able to demonstrate a direct relationship between platform processes and the potential for harm to be caused by them, when companies continue to share limited or insufficient information about how their services are actually designed and run.

Understanding the experience of all children

The regulator should have a specific duty to assess the risk of harm to particular groups of users, and to assess how online harms may be disproportionately experienced by them. This should include a consideration of how online harms may be differentially felt by users with one or more characteristics under the Equality Act.

Provision should be made for the regulator to be informed by a wide plurality of user experience. We recommend that the regulator develop user representation structures for this purpose, enabling it to inform its approach to engagement with those that have experienced online harms, and represent a broad cross-section of UK users (including those that may be exposed to risk on an intersectional basis.)

Similarly, the regulator's research programme must ensure it captures the plurality of children's experience.

Children are likely to experience online harms in many different ways. For example, during the first lockdown concerns were expressed that children with long-term health conditions were being targeted online, including children with epilepsy being targeted with content designed to trigger seizures.[44]

Similarly, there is extensive research which suggests that LGBTQ+ children are likely to face greater levels of harassment and abuse online, and are more likely to be contacted by people online who aren't who they claim to be.[45]

[42] Ofcom will have a specific duty of promote innovation through the Online Safety Bill

[43] The value of funded user advocacy arrangements is set out well by Citizens Advice in their assessment of sectoral regulators. Citizens Advice (2018) Access denied: the case for stronger protections for telecoms users. London: Citizens Advice

[44] Based on discussions with the Epilepsy Society

[45] See for example, McGeeney, E and Hanson, E (2017) Digital Romance: a research project exploring young people's use of technology in their romantic relationships and love lives. London: Brook/CEOP

Next steps

It is vital that the Government Introduces the Online Safety Bill as soon as possible. We encourage Government to publish a draft bill in spring 2021, and to have a legislation on the statute book in early 2022. In turn, this should enable Ofcom to establish its regulatory scheme and begin making its first regulatory decisions shortly afterwards.

Although the scale and complexity of online sexual abuse has been increasing for several years, the importance of online harms regulation has been brought into sharp focus during the Covid 19 pandemic.

The failure to design often basic child protection measures into their services and invest sufficiently in technology that could disrupt abuse, meant that many social networks could be readily exploited by abusers looking to capitalise on the 'perfect storm' that the pandemic created – children spending longer online, more content needing to be moderated, and sustained pressures on moderation during both the first and second waves of the pandemic.

But the increased risks to children will not disappear once the crisis begins to subside.

As a result of the pandemic, children have changed the way they socialise and learn; we've seen the mass adoption of video chat and livestreaming technology, with companies rushing out new products to chase market share, but with very high-risk design features in terms of grooming; and with long-term changes to working patterns likely to result in higher demand for child abuse images, and an increase in grooming to fuel it.

Children have long needed comprehensive and ambitious action to protect them online, but with the pandemic likely to result in structural changes to the child abuse threat, there is an unarguable case for the Online Safety Bill to do all it can to protect children from inherently avoidable harm – both now and well into the future.

Prior to legislation being passed, it is vital that both the Government and Ofcom use all the levers at their disposal to deliver safer online environments for children.

We strongly welcome the Government's publication of the interim Code of Practice on online child sexual abuse. This sets out the steps the companies in scope of future regulation should take to mitigate the risks that abuse takes place on their platforms. The code itself is voluntary, but in conjunction with the voluntary principles for tackling child abuse agreed by the major tech firms and the Five Eyes governments in March 2020, it gives a strong steer for companies to put in place systems and processes to protect children from harm.

However, we have not yet seen what steps, if any, companies have taken or will take in the near future to comply with either the codes or voluntary principles. We encourage companies to publish an assessment of the changes required to their current policies and processes to achieve compliance. The Home Office and relevant Select Committees could usefully monitor which policies companies are planning to adopt in the interim, and how they might work in practice.

As a precursor to online harms regulation, Ofcom can and should now look to adopt a robust enforcement approach to video sharing platforms (VSPs), in accordance with its duties as the regulatory body for the Audio Visual Media Services Directive in the UK. Although platforms such as Facebook and YouTube will be regulated out of Dublin, Ofcom will regulate a number of large VSPs, likely including Twitch, Snapchat and TikTok.[46]

Platforms likely to be in the scope of online harms regulation will be keenly observing Ofcom's risk appetite and enforcement approach, making an active enforcement approach important in focussing minds ahead of the Bill coming into force.

Finally, both Government and Ofcom should continue to invest in strategies to support compliance across companies both large and small. DCMS should ensure its safety-by-design framework is a compelling and valuable tool to support the embedding of better product safety choices; and that the safety tech sector continues to receive much-needed support to develop innovative safety solutions – ensuring size is no barrier to an online service being able to discharge its Duty of Care.

In the coming months, the Government and Parliament will take decisions on the shape of a Bill that has the potential to deliver a world leading regulatory approach, and that will be a crucial part of the child protection system for decades to come.

If it is suitably bold and ambitious in its approach, the Government can deliver on its laudable objective to make the UK the safest place in in the world for a child to go online.

We should settle for nothing less than an Online Safety Bill that prevents avoidable harm to children, and gives young people the protections they deserve.

[46] Ofcom (2020) Video sharing platform regulation: call for evidence. London: Ofcom

Appendix one
Scorecard against the NSPCC's six tests

The NSPCC will use a scorecard approach to assess whether the Online Safety Bill and Ofcom's regulatory scheme meets our six tests for effective regulation.

Against each test, we set out a series of indicators that will determine whether regulation goes far enough to protect children from avoidable abuse.

Across nine indicators, the Government has either met our position or we are broadly satisfied with the developing position.

At present, we consider that nine out of 27 indicators are wholly or largely unmet.

Key:

🟢	*indicator wholly or largely met*
🟡	*indicator partially met or still to be determined*
🔴	*indicator wholly or largely unmet*

Test one: the Duty of Care

A fully-fledged Duty of Care that requires platforms to take a systemic approach to protecting children, through the identification of reasonably foreseeable harms and proportionate measures to address them	🟢
Codes of Practice are intelligently designed, setting out ambitious but deliverable expectations for the discharge of the Duty of Care	🟡
Ofcom's regulatory scheme corresponds to the scale of online harms children face, with platforms incentivised to respond to current risks (and notify the regulator of emerging ones)	🟡
The Government adopts, as one of the guiding principles for the regulatory framework, an objective for Ofcom to incentivise cultural change through the development of its regulatory scheme	🟡

Test two: tackling online child abuse

Ofcom is enabled to deliver a regulatory scheme that requires bold and ambitious action on child sexual abuse	🟢🟡
Ofcom demonstrates a clear understanding of the child abuse threat, and emphasises the prevention of avoidable harm is a central focus of the regulatory approach	🟡
There are clear and comprehensive expectations on platforms to address how their design features exacerbate child abuse risks, including high risk design features	🟢🟡
There are specific requirements to disrupt online grooming, remove illegal content in a child centred and consistent way, and to take steps to prevent the production and distribution of new child abuse images	🟢🟡
There is a regulatory duty on Ofcom to address the cross-platform nature of risks, with corresponding requirements on platforms to share data on offending behaviour and threats	🔴
The Online Safety Bill ensures an upstream approach to tackling child abuse, with the regulator treating content that facilitates illegal behaviour with the same severity as material that meets the criminal threshold	🔴
Private messaging is in scope, recognising it is a major driver for the production and distribution of child abuse images and grooming	🟢
The regulator has proportionate but effective mechanisms to address and mitigate the impacts of the highest risk design features, including end-to-end encryption	🟡

Test three: tackling legal but harmful content

The regulator develops a comprehensive and highly effective approach to tackling legal but harmful content, recognising its significant impact on children's safety and well-being 🟡

Ofcom produces a Code of Practice that clearly sets out what it considers an acceptable response to priority categories of harmful content. This should include moderation strategies, how content is algorithmically recommended to users, and what it considers suitable outcomes from age assurance measures 🟡

The scope of the Online Safety Bill is amended to capture all commercial pornography sites 🔴

Test four: transparency and investigation powers

The regulator has comprehensive investigatory and information disclosure powers 🟢🟡

Annual transparency reports provide meaningful and intelligible information on the scale and extent of abuse risks, and the effectiveness of response 🟡

Ofcom is appropriately resourced to conduct thematic reviews and investigations, and has a strong risk appetite for doing so 🟡

Category one services face broad but workable information disclosure duties, including a proactive duty to disclose information about which the regulator could reasonably be expected to be aware 🔴

Category one services are required to 'red flag' significant breaches of the Duty of Care that compromise children's safety or put them at risk 🔴

Test five: enforcement powers

The regulator has a suitable range of enforcement mechanisms for companies, including robust financial sanctions 🟢

The regulator is able to use a range of intelligently designed and proportionate business disruption measures 🟢

The Government commits to senior management liability that is directly linked to the discharge of the Duty of Care, and that is able to secure the extent of cultural change that is required. Senior managers are personally accountable for decisions on product safety, not only a failure to cooperate with the regulator 🔴

Managers exercising a 'significant influence function' are liable for regulatory action if they breach their Duty of Care requirements, with the option of criminal and financial sanctions for the most egregious breaches 🔴

Test six: user advocacy arrangements

The Government commits to a user advocacy body for children, funded by the industry levy, to ensure a 'level playing field' for children, and ensure children's interests are represented in regulatory decisions 🔴

There is an effective supercomplaints process for systemic breaches of the Duty of Care to be investigated 🟢

There should be a duty on Ofcom to assess the risks of harms to particular groups of users, and assess how online harms maybe disproportionately experience by them. This should include an assessment of how online harms may be differentially experienced by users with one or more protected characteristics under the Equality Act. 🔴

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 here to make children safer right across the UK.

nspcc.org.uk

EVERY CHILDHOOD IS WORTH FIGHTING FOR