Online Harms White Paper Response

Organisation responding: The UK Safer Internet Centre

Contact details of person responding: Kate Jones, Deputy CEO at Childnet, part of the UK Safer Internet Centre. Tel: 020 7639 6967. katejones@childnet.com

About the UK Safer Internet Centre

We are a partnership of three leading organisations: Childnet International, Internet Watch Foundation and South West Grid for Learning (SWGfL), with one mission - to promote the safe and responsible use of technology for young people.

The partnership was appointed by the European Commission as the Safer Internet Centre for the UK in January 2011 and is one of the 31 Safer Internet Centres of the Insafe network. The centre has three main functions:

- Awareness Centre: to provide advice and support to children and young people, parents and carers, schools and the children's workforce and to coordinate Safer Internet Day across the UK.
- Helpline: to provide support to professionals working with children and young people with online safety issues.
- Hotline: an anonymous and safe place to report and remove child sexual abuse imagery and videos, wherever they are found in the world.

The UK Safer Internet Centre is funded under the Connecting Europe Facility (CEF) programme of the European Commission. As such we contribute to the Better Internet for Kids (BIK) core service platform to share resources, services and practices between the European Safer Internet Centres and advice and information about a better internet to the general public. In line with the European Commission's Better Internet for Kids strategy, the key vision behind the BIK core service platform is to create a better internet for children and young people.

Introduction

We broadly welcome the Government's Online Harms White Paper and the opportunity to contribute to the new proposed regulatory framework. We particularly welcome action taken by both the Home Office and Department for Digital, Culture, Media and Sport to ensure that there are high levels of engagement with industry stakeholders and others, and for affording the UKSIC and its three member organisations the opportunity to contribute to those discussions.

Our response to this consultation is focused in part on three crucial areas of concern to UKSIC in this White Paper:

- **Defining the Scope and Harms-** Further work and clarity is needed from Government in several important areas. This includes further defining 'harmful' content in scope of the White Paper with regards to the response required to it and its impact. This is particularly with reference to online harms that are "less clearly defined".
- **Education and awareness raising-** around online safety and online harms is crucial and needs support from Government to ensure that sufficient importance is placed on it in formal education settings, and that there is support for education and awareness raising more broadly. Education and awareness raising can help prevent online harms by educating the public about their rights in an online context, and in supporting users to develop positive online behaviours, thereby preventing risk and harm taking place. Platforms and services must also contribute in this space. There is a particular need for more support for education, training and awareness raising in schools.
- **Provision of services to the Internet Industry-** UKSIC members are already offering services and support that are crucial in delivering the desired outcomes of the White Paper.

- **The IWF** works to minimise the availability of illegal content online- specifically child sexual abuse images and videos. The IWF provides an anonymous place for the public to report suspected CSAM and utilise the latest technology to proactively search the internet for this content.
- **SWGfL** runs a support service – Report Harmful Content Online – that exists to support users through online reporting systems and offers mediation, support and escalation for individuals who do not get the outcome they hoped for through reporting processes on online platforms.
- **Childnet**, in its work as the awareness centre of the UKSIC, produces educational content and support that reaches hundreds of thousands of teachers, young people, professionals and parents each year, and co-ordinates Safer Internet Day in the UK. These services and support will continue to have an important part to play and we are looking to Government to further use the insight, expertise and reach of the UKSIC in delivering its outcomes.

Question 1:

This Government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the Government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

Agreed definitions

Government should set out clearly, using a robust evidence base, agreed comprehensive definitions of the online harms as set out on page 31 – Table 1 'Online harms in scope'. It is imperative that industry, civil society and users know clearly what is in scope of the regulator and what will be addressed under any new regulation. Clear definitions based on evidence is essential as a foundation to build a culture of transparency, trust and accountability. This is particularly important for those harms with 'a less clear definition'. Where the Online Harms White Paper states that the list is neither exhaustive or fixed, it should be made clear how new harms will be identified and responded to. Where certain online harms will be covered under other bodies, government or otherwise, this should be clearly communicated to users.

As part of its work in the UKSIC, SWGfL has developed information, support and mediation to all UK users (over 13 years old) with regards to legal but harmful online content through its ReportHarmfulContent platform. The service provides definitions of what legal but harmful online content is – these definitions would contribute towards the work started on page 31 – Table 1 of the White Paper.

Clear standards

The new Regulator should be responsible for setting principles about what companies are expected to do and how they are expected to do it, using a more standardised approach to reporting online harms as part of this. The Regulator should also set standards for how content is managed, based on reasoning and proportionality, balancing rights and ensuring accountability for decisions. The Regulator also needs to consider the obligations that transparency reporting would place on companies of all sizes in scope of the White Paper.

Two key principles we think the Regulator should be tasked with are:

1. Clearly setting out the responsibilities of the companies around transparency.
2. Assessing what processes they are deploying and communicating to tackle online harms on their services, and what impact they will have with the public and Parliament.

Transparency and accountability

UKSIC welcomes the measures to increase transparency outlined in the White Paper. We feel that transparency is important:

- for accountability of the service provider
- for informing users and developing user trust
- to build up a picture of the scale of the challenge that companies face in tackling illegal and harmful content on their platforms.

Transparency and reporting

One area where transparency data can bring greater accountability is the reporting system. Users need confidence in the system, and for this all providers should fulfil – and provide data around how they are performing against – certain best practice standards, including:

- acknowledgement of receipt of reports, as well as
- setting users' expectations as to likely timings of the report being dealt with,
- giving users feedback about the outcome of a report, (proactively giving this feedback to the user directly, rather than the user having to search for this result within the platform)

- providing in-line reporting tools and
- offering additional signposting and advice (whether or not any action has been taken).

These are all key for users to feel confident in the reporting process, and we expect these to be included in the codes developed by the regulator (and were included in the draft codes in the Government response to the Internet Safety Strategy Green paper (pp64-65). The hope is that this will bring consistency across platforms and improved reporting tools.

Transparency and numerical data

The UKSIC supports transparency reporting by online services in scope of the Paper to illuminate the performance of platforms against agreed standards, and the reports they process. The areas covered in 3.17 where the regulator has the power to require annual reports from companies are sensible. We would suggest care in constructing numerical reporting indicators, and that there needs to be a focus from the regulator on processes and how a company identifies, assesses and removes illegal or harmful content on its platform, rather than just on the volumes or large numbers. For example, a high number of reports on a service can reflect an effective reporting system where users have confidence in the system and are motivated to report, just as much as it can indicate a service where perceived breaking of the rules is the norm.

Equally, comparing the number of reports to the number of takedowns isn’t an effective way to draw conclusions about a service’s reporting / moderation if used in isolation. Care is also needed to avoid influencing providers to make amends to their reporting policies or processes that are to improve ratings rather than in the interests of their users. As an example a measurement of report closure rates; providers may choose to focus on closing reports more rapidly to increase their performance, however this may be to the detriment of their users and user experience.

If there is a way to look at how long a moderator is able to spend looking at a piece of content, we believe that could be useful – for example, what is the average length of time before making a decision. Clearly this will also differ for different types of content, video for example.

Transparency and access to data

The development of transparency data is important, but the data only brings transparency if it is read and used. The UKSIC would like to see transparency reports viewable by all, as well as presented to the public in a digestible way by both online services and the regulator.

It may not be likely that users will read the reports of all the services that they or their children are using, so clear thought should be given to ensuring that this data has the desired effect, and is understood correctly, and education and awareness is vital here. Data from transparency reporting will be important for informing education and awareness work, which seeks to empowers users to use online services safely and responsibly.

What more can be done?

Effective reporting systems (of online service providers) are crucial for ensuring users’ safety on social media, gaming sites and messaging services and key to this is user confidence in these processes. UKSIC agrees that all service providers have a duty of care to remove and reduce inappropriate behaviour or content on their platforms. Areas for improvements we can recommend here, that would fall within the regulator’s remit as it works to draw up code of practice and standards, include:

- Ensuring there is no systemic failure with reporting
- Recognising that content review decisions are not always straightforward
- Future-proofing reporting
- Blocking of sharing of content that has already been deemed to be illegal or harmful, between different platforms

- Transparency about other measures services are taking to improve safety on their services, to share best practice
- Technological tools in transparency, e.g. the SWGfL tool – http://testfiltering.com - that can be used by the public or organisations to test to see if their internet connection is using the IWF blocked list as well as CTIRU.
- Contribution towards public education around terms and conditions and the reporting process
- Contribution towards public education around expectations and duty of services
- Structures to bring industry, companies and non-governmental stakeholders together to discuss challenges and issues, where companies feel like they can open up about issues on their platforms and get support to solve them

Question 2:

Should designated bodies be able to bring 'super-complaints' to the Regulator in specific and clearly evidenced circumstances?

Yes.

Question 2a: If your answer to question 2 is 'yes', in what circumstances should this happen?

Clarity about who can report to the regulator, and under what circumstances is a crucial part of public confidence in the new regulatory system.

The UK Safer Internet Centre is pioneering work in this area, with its dedicated helpline for professionals working with children and young people (POSH), run by SWGfL, and the SWGfL launching its ReportHarmfulContent reporting hub in late 2018 to support victims facing legal but harmful online content.

ReportHarmfulContent reporting hub provides information, support and mediation to all UK users (over 13 years old) with regards to legal but harmful online content. The service provides definitions of what legal but harmful online content is; support for users facing these issues, and direction of how to report these issues to social media and online service providers.

Should a user have reported their issue and received a null or an unsatisfactory (from their perspective) response from the social media or online provider, ReportHarmfulContent will assess the case, working to establish the context in order to determine if the response to the original report was unfair. If the response was fair, the user will be provided with advice and an explanation. If the conclusion is that the response was unfair, ReportHarmfulContent might either provide further direction or accept the case and represent the claimant with the social media or online provider. In the 6 months since launching ReportHarmfulContent, of the cases accepted, 87% have resulted in the harmful content being removed.

ReportHarmfulContent is a primary example of a designated body that could bring 'super complaints' to a regulator, as well as the other SWGfL support helplines, including the Revenge Porn helpline, the UK's only service dedicated to supporting all adults who have been victim of intimate image abuse. Victims would benefit from having strengthened their complaint and bring some further redress for what is likely to be a distressing situation.

Super-complaints would clearly be a helpful step in understanding the scale of an issue. Whilst super-complaints are helpful there would need to be clear advice and guidance provided to those seeking to make super-complaints and it may be helpful to limit these complaints to those with specific expertise working in these areas, such as charities and law enforcement agencies.

Question 3:

What, if any, other measures should the Government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

For users who have concerns

- **Making reporting easier:** More education is needed on reporting across the different platforms as users are using multiple platforms (often simultaneously) that have a variety of different functionalities. Government should encourage consistency in the reporting process across platforms, particularly when the services offered are similar.
- **Clarity on the role of the regulator:** The regulator will have an important role to play, but it is important to be clear on the limitations of the regulator, and to make sure that people understand the way in which the regulator can help them.
- **Providing a process for users to raise a complaint:** It is important for all users to have a process for raising a complaint if they are not happy about how a report has been handled and if they want an independent arbitration.
- **Enabling reporting for non-account holders**
- **Clarity and transparency for those who are reported against:** Support for those whose content who is taken down, or where action is taken against a user, is also important. This is particularly important if those who are reported are young people themselves and unaware of why their behaviour has breached the platforms standards, or are at risk themselves. For example young people (particularly those with SEN) are not always fully supported or fully cognisant of the impact of their behaviour, and taking down their content or suspending their account in isolation, without support and education, will not change their behaviour but potentially isolate them even further.
- **A route for redress**: The UKSIC, through the SWGfL's Helpline Services already provides support and can work to continue in this capacity, given funding to do so.

Education and awareness on harmful content and how to report

- **Education about what to report:** There is the need for education for users about what is not OK online, and what people should report, as well as that it is worth making a report about harmful content.
- **Education about how reporting works:** This would include being clear about the anonymous aspects of reporting for example, education on how best to report, and identifying the barriers young people face, and taking steps to overcome these. Education will have an online and an offline component.
- **Support reporting offline:** it is important to think about the offline support that can be offered, and this includes in the instances where the content is not taken down. Signposting to other related organisations that can help, for example, ChildLine or the Samaritans.
- **Listen to users on reporting:** Regular research with users, particularly examining awareness and confidence in reporting mechanisms, will help to inform both the Codes and the additional needs in this area, recognising that these needs may fall outside of industry reporting.
- **Better police response to victims of crime online**: through education and awareness raising amongst police forces alongside the capacity and funding to respond adequately
- **Training for professionals working with children**: as a high degree of issues are reported via schools and established child protection and safeguarding process, those working with them need be able to access training to ensure competency in their ability to recognise, respond to, and resolve issues related to online harms with under 18s.

Question 4:

What role should Parliament play in scrutinising the work of the Regulator, including the development of codes of practice?

Parliamentary oversight

We agree with the suggestion that the Regulator should be independent. Parliamentary involvement should only be in an oversight capacity and the regulator should remain independent, providing reports on a regular basis. Parliament also has a role in the protection of free speech and ensuring that the rights of individuals to a private life are also balanced against the safety needs of children.

It is important the work and impact of the regulator is reviewed and evaluated regularly, particularly due to the fast-paced changing nature of digital technologies.

The regulator should remain independent of Parliament with regards to how it identifies online harms, as this should be ascertained from a robust evidence base including consultation with online services and non-governmental stakeholders such as the UKSIC working in this space directly with children and young people around new and emerging harms.

The regulator must remain politically independent. We do see the potential for a public scrutiny role for Parliament, perhaps through the use of Select Committees, to test Codes of Practice with public sentiment around harms, scrutinise senior appointments made by the Regulator, the work of the Regulator and in scrutinising the budget of the Regulator. Technical knowledge and expertise will be vital to the role of the new Regulator, and as such Parliament is probably not best placed to assist in the development of codes of practise. Rather, this role should be left to the Regulator, industry and other technical experts.

Codes of practice

The codes of practice need to be practical, based on evidence gathered from a variety of stakeholders, and reflect the needs of the users in relation to the technology they are using. Care should be taken that the codes work to enhance the services through safer provision, and enable industry and the regulator and other organisations to collaborate over this work. This collaboration can assist in helping the development of the codes which can help in the codes then being more transparent, and there are also advantages in such collaboration leading to support in any explanation and communication about the contents of the codes.

We would like to see a duty placed on either the Home Secretary or the Regulator to consult relevant experts such as the UKSIC in the development of the codes of practice.

Question 5:

Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

In principle, UKSIC broadly supports the intent of the proposals in the White Paper. However, there are some key areas which require further examination and clarity.

Clearly, the range of services in scope is significant and will require serious capacity to address within industry – an issue that could affect smaller companies disproportionately. Online services are different to each other, and some areas of online harms outlined in the White Paper are more challenging to manage than others, and clarity is key here to effective industry action and compliance.

What is important from a user perspective is that users' expectations of services that they use are uniform and accurate – ensuring for instance that content that is deemed harmful on one platform would also be considered and dealt with in a similar way on another.

In this context, the regulator will need to agree a broad set of principles rather than a granular duty of care and, if this is the case, it would be difficult for a regulatory body to enforce removal of harmful but not criminal content. This makes support mechanisms such as the SWGfL's ReportingHarmfulContent platform crucial in supporting users experiencing harmful content.

Areas of concern

Private communications: More clarity is needed around private communication and what is included in the 'tightly defined categories of illegal content'. The Government must also pay careful attention to current laws and legal frameworks in this area including Article 15 of the e-commerce directive and Article 12 on the UN Declaration of Human Rights, which safeguards an individual's right to be free from interference with their privacy, family, home or correspondence. One way the Government could begin this discussion would be to focus on the issue of User Generated Content (UGC) which is a manageable and understandable definition to start from.

Private and encrypted services: There is a need to examine how safety and encrypted services can work together, to identify the optimal balance between privacy and safety, and that all possible safety measures within such private services are known and where possible implemented. If private communications are outside the scope of the regulator and this White paper, there is the real risk that there is an incentive to some service providers to move to a more private model. If this could help avoid regulation, there is the risk of establishing perverse incentives for more services to use end to end encryption.

Gaming: We would recommend that online gaming and apps are explicitly mentioned, as this area falls clearly into the definition provided – 'services or tools that allow, enable or facilitate users ….. to interact with each other' p49.

Question 6:

In developing a definition for private communications, what criteria should be considered?

Defining private communications can be challenging. We would recommend that this is defined in collaboration with industry and organisations working in the field of online safety such as UKSIC alongside the ICO to ensure a thorough understanding of the complexities of privacy.

The UKSIC recommends that the following factors be taken into consideration as the definition is developed:

Multi-functional services: some platforms offer users the ability to both post publicly and communicate privately using the same 'brand' – e.g. Facebook, has Facebook Messenger, private communications channel operating on a public social media platform. From a user perspective, having differing standards and codes across these functionalities would cause confusion and greatly undermine efforts to improve trust, transparency and accountability. UKSIC would recommend in this case that the more that all services can be encompassed by the regulatory regime, whether considered private or not, the easier it will be to the end-user and others.

Encryption and users: Defining encrypted services as 'private' and leaving them outside the scope of the White Paper may have unintended consequences such as encouraging companies to opt for encryption to avoid being in scope, as well as those intending to cause harm through for instance grooming, child sexual abuse or hate speech moving onto services that are outside the scope of the White Paper

Technical considerations around encryption: An emerging challenge for the new regulatory framework will be to consider how the Regulator will deal with the technological trend for greater levels of encryption and user privacy. DNS over HTTPs for example, if implemented, in its proposed form, could have a catastrophic impact on the ability to block illegal child sexual abuse content through ISPs. It could lead to complications with the enforcement of the Government's age verification policy on adult pornographic websites and would also have implications for the blocking of terrorist content and copyright, as well as parental controls currently offered when a customer sets up their broadband connection with any of the major ISPs operating in the UK. Equally, schools will experience the same impact and challenge. Specifically, for schools in England and Wales, the challenge will be in meeting their statutory obligation to provide appropriate levels of filtering. Companies will only be able to deploy technical services to disrupt the distribution of illegal images if they can see what activity is being conducted on their platforms, which is why the Regulator and government will need to carefully consider the impact of end-to-end encryption, DNS over HTTPs and other privacy issues and ensure that this is not at the expense of child safety requirements.

Private group chats: Some private communications can be very public when there are groups involved, and end-to-end encrypted services can fall into the definitions of social media. There are real challenges in drawing lines between services or within services, and any lines will make the regulatory regime harder for the end-user to comprehend, which runs the risk of it becoming less effective in keeping user confidence. Certainly, a range of services can be involved in the online harms identified, and in some case, such as online grooming, this can move from more public to private communications (where the offender might feel safer).

Question 7:

Which channels or forums that can be considered private should be in scope of the Regulatory framework?

We would also recommend that this particular question is consulted upon with industry as well as organisations working in online safety such as the UKSIC, to ensure that those services that are considered to be in scope will be able to adhere to the regulatory framework. We would recommend the widest possible scope to avoid public confusion with some services being out of scope, leading to risks that the regulatory regime could be undermined.

Hyper local channels: We would recommend that hyper-local channels (e.g. airdrop and Bluetooth) be included within the scope. These channels are often used to share harmful content and in particular illegal content (e.g. intimate images or copyrighted content). If hyper local services fall outside of the scope of this White Paper, it needs to be clear where this lies.

User expectations across different services: The expectation from the public's perspective, who wish to report harmful content or behaviour, will be that the same rules apply on all services. For example the user experience in using WhatsApp Status updates is very similar to using Instagram Stories, even though the former uses E2E.

'Private communications' with large groups: The same problems of confusion would exist if lines are not only drawn between services, but within services – i.e. if a group on a private network has above a certain number of members.

Question 7a:

What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

Reporting: Clear, prominent, accessible reporting functions should be available for users. Reporting should automatically (very easily) share with the service provider a screen grab or the message trail, to allow for effective review.

Transparency: private services should be included in the regulator's requirements around transparency, and they should need to demonstrate to the regulator what they are doing to keep their users safe.

Quicker response times: There needs to be a quicker more streamlined process for sharing information in emergency situations to enable law enforcement to gather the evidence they require in order to make a prosecution.

Training for professionals: understanding amongst social workers, police and health should be improved.

Parity with 'non-private' channels: The powers of investigation must be the same across all services regardless of privacy, rather than a trade-off between privacy and safety.

Review of support available: We would like to see a systematic review as to how to support users of private networks to have a private and a safe experience. This would include a discussion and recommendations around the balance between safety and privacy, and Parliament might have a role in this, as regards balancing users' rights to freedom of expression with the safety needs of all users and particularly vulnerable users and young people.

Question 8:

What further steps could be taken to ensure the Regulator will act in a targeted and proportionate manner?

The UKSIC supports the clear mention of the rights-based approach in 5.12 and the obligation to support innovation 5.11. It is essential that the Regulator operates a principles-based approach with proportionate action. Government needs to be clear about the parameters of the duty of care to ensure effective regulation, with the regulator having a comprehensive understanding of the complexities surrounding online harms.

If parameters are not clearly defined this may have a negative impact upon relationships with industry and lead to uncertainty about when a breach of the new regulatory framework has occurred. The regulator will have a key role in making sure that the regulatory system works, and that the measures required are adoptable by all those that fall under the remit.

We recommend collaborative working between industry and the regulator. The regulator should also have clear mechanisms in place to consult widely in the online safety sector including with helplines (such as ChildLine and POSH). Both these strategies will be of particular value when emerging new threats or issues arise which are in the public interest. For example, the Christchurch call, or in the case of ‘Momo’ as reported by The Guardian, worries around the ‘Momo challenge’ spiralled as legitimate concerns about online harms were exacerbated with little evidence to support them.

Question 9:

What, if any, advice or support could the Regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

We want to encourage safer online services, and for them to have practical advice on how to comply with the existing duty of care and make sure their users are safe on their service. The regulator should make it clear what it expects, as well as giving clear indications in a practical way on how its expectations can be met. The issues relating to online safety go beyond the harms outlined in this White paper, and we would encourage a broader level of support beyond compliance to be provided, and ensuring the wider online safety needs of users, especially young and vulnerable users, and those who support these, are fully taken into account.

Support forum: The regulator should provide a forum where start-up companies – as well as larger ones - are encouraged to disclose issues with their platforms or the design of them, in order to get assistance to design in safety during development of new platforms or updates to existing ones. This should be based on a flexible, principles-based approach that sets reasonable expectations of a small company.

Identifying emerging harms and technical challenges: The Regulator will be vital in researching and identifying these trends and working with the industry to designing technical solutions to future challenges. The scale of this task should not be underestimated, and this will require significant resourcing in areas which may never actually emerge as issues.

Ensuring the regulatory system is practicable: The regulator will have a key role in making sure that the regulatory system works, and that the measures required are adoptable by services in scope of it.

Self-assessment tools: These would support online services to identify where they need to improve or focus, particularly for smaller companies. SWGfL have developed such tools for schools, with the result that over half of schools in this country use 360 Safe.

Question 10:

Should an online harms Regulator be: (i) a new public body, or (ii) an existing public body?

Question 10a:

If your answer to question 10 is (ii), which body or bodies should it be?

UKSIC has no strong view on this, however, we recommend that the Regulator will need to have:

a strong relationship with the industry it is regulating

to be able to understand the technical and legal complexities of the online environment.

a strong working knowledge and understanding of regulatory frameworks

an understanding of how it works in partnership with other regulators

It would be our view that the Government should be seeking to utilise the current skills and expertise of regulators and experts already operating in this space to drive meaningful change, even in the period whilst the legislation is being passed. We would favour at least initially, a regulator that already has a relationship with the industry and whose powers could be expanded to cover online harms, with a review and a move towards a new regulator over time if that were deemed in the best interests of internet users.

Question 11:

A new or existing Regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

UKSIC has no fixed viewpoint about the financial modelling of the Regulator.

However, we would encourage clear consideration on the importance of industry funding for other key areas that are essential for keeping children safer online. Education and awareness, the empowerment of young people and those that support them (parents, teachers and other professionals that work with children) is crucial. Removing the capacity of industry to donate to voluntary initiatives could be severely damaging – for instance impacting the number of indecent images of children removed by the IWF, increasing the workload on an over-stretched and struggling law enforcement system, and hindering international collaborative work with INHOPE. Increasing the amount of industry contribution to the area of supporting online safety could be one answer, including for education and awareness around those areas of online safety that are of concern to young people but outside the scope of the White Paper, such as peer pressure, mental health, and body image.

The UKSIC operates thanks to a 50% funding contribution from the EU, and industry contributions either financial or in-kind are therefore vital to our work. Safer Internet Day in the UK, for instance, is the biggest national online safety awareness campaign in the world, and it is growing each year, reaching almost half of 8-17 year-olds in the UK in 2019, and over a quarter of parents with online safety messages. The concern we have as UKSIC is to ensure that industry recognise and are able to meet this need, whilst also meeting any requirements to support the regulator.

Consideration of any requirements on industry to fund the regulator should also be given to how the future funding model will ensure the UK Safer Internet Centre and its three partners can continue in their vital roles.

Question 12:

Should the Regulator be empowered to i) disrupt business activities, or ii) undertake ISP blocking, or iii) implement a regime for senior management liability? What, if any, further powers should be available to the Regulator?

The regulator should have the power to remove illegal content, and the power to issue improvement warning notices to the industry. It should be responsible for reporting publicly on the effectiveness of companies at dealing with issues of harmful and illegal content on their platforms.

The UKSIC does not have a fixed view on the wider powers of the regulator mentioned above, but we believe that it is good to be exploring all of the options and powers mentioned in the White Paper.

We would recommend that this will need to be decided on a case by case basis as one model will not fit all scenarios. If, for instance, the regulator can remove harmful but not illegal content, this will need to be defined in the statutory duty of care industry are to abide by and until this duty of care is defined it is difficult to say which sanction(s) would be the most relevant. There is also the issue of whether a company has its jurisdiction outside the UK, which may limit the powers of the regulator or define what actions can be taken in response to breaches of the duty of care.

Question 13:

Should the Regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

The UKSIC does not have a fixed view on this, beyond highlighting that in deciding whether or not a company based outside the UK / EEA should appoint a representative in the UK / EEA, the Government should take into account any potential unintended consequences affecting the decisions that companies need to take about locating their business within the UK.

Question 14:

In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the Regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

Question 14a:

If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

Question 14b:

If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

The UKSIC recommends using the judicial review system already in place as it is an appeals process in itself. We have no fixed view on the circumstances in which companies would be able to use this, or the bases on which the appeal should be decided.

Question 15:

What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Opportunities for innovation

AI: this is already being used as a tool for good in some respects and the regulator could take a lead in bringing together stakeholders in industry and those working with users on the ground who understand the issues they encounter online, to build new technologies that use AI to support legislation.

Collaboration: Using the new regulator and new regulatory environment to bring safeguarding / safety expertise together with innovators and start-ups; joining up these 2 teams from the start there is a better chance for safety by design to be implemented in the initial development phase.

Opportunities for adoption of safety technologies

Gamification: gamification of safety features would ensure appeal to younger users and contribute towards education around safety and reporting.

IWF Hash list: UKSIC would recommend that all social media and online providers utilise the technologies available to identify and prevent illegal and harmful content (images and video) to be uploaded, specifically the use of the IWF Image Hash list

Barriers to adoption of safety technologies

Uncertainty around funding: Uncertainty surrounding Brexit is the cause of challenge for the UKSIC. UK Safer Internet Centre partners are in receipt of European funding to maintain many vital national services and their continued contribution is at great risk. There has been in the UK a lot of work done by the partners in the UK Safer Internet Centre, for example, in the hotline (IWF), the helplines (POSH and RHC run by the SWGfL), youth participation (for example Childnet's Digital Leaders programme) and awareness (Childnet and SWGfL) including the organising of Safer Internet Day in the UK. Each year our collective work grows, as does our impact, and the continuity of EU funding for the UKSIC has been crucial in this. Government has a key role in ensuring the continuation of funding, to continue the development of momentum for this crucial work on a national level, which in turn will enable innovation in these areas.

Encryption: encryption of services could make it harder to retrieve information.

Question 16:

What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

Age Verification: if it can be made to work effectively, it would make sense to deploy this across all services in scope to allow them to prevent underage users from accessing their platforms. UKSIC is well placed to provide practical guidance to organisations about safety by design with regard to young people.

Violence against women and girls: It is apparent from the work of the UKSIC across helplines, hotline and awareness centre that violence against women and girls accounts for a large amount of illegal and harmful content, and we propose that guidance is issued in this area specifically.

Image and video hosting platforms: UKSIC recommends support to prevent illegal images from being uploaded by using hashing technologies. For example, UKSIC would like to see social media and online providers utilise the IWF hash list to prevent known illegal CSAM images from being uploaded.

Extremist content online: The area of extremism and radicalisation is complex and hard for online services to filter and make decisions about. More support from Government, academics and experts is needed, particularly with regards to definitions, search terms and illegal image and video identification.

Support / funding for start-ups: safety often costs funding that a level of success/popularity will enable, so market forces dictate that a new online service can only ‘afford’ safety by design once it is popular, which is contrary to the aim of safety by design. Work is need to redress this, and we see an opportunity for government and the regulator to support in this space. Clearly making safety a marketable asset is important in the response here, as safety can help bring success in this way.

In developing practical advice, the Government should draw on the expertise of the UK Council for Internet Safety, as well as relevant stakeholders such as ICO, BBFC and IWF, for example, as well as involving the UKSIC.

Question 17:

***Should the Government be doing more to help people manage their own and their children's online safety and, if so, what*?**

Everyone has a role to play in ensuring that users including children are safe and happy online. Children and young people need to be aware of their rights online and government has a key role to play here.

Both equality of access and the safe, healthy and happy use of the internet for children can be achieved through: education; children's participation; legislation and regulation of businesses using digital media; supporting parents/caregivers and wider community networks; cross-sectoral and government department working and responses; ensuring policy approaches are evidence-based; transnational working; awareness raising for children so that they know their rights; emphasis on digital literacy and citizenship from an early age; and child centred information online (health, education etc.).

UKSIC delivers an intensive programme of online safety education and awareness raising in schools and with professionals working with children, a helpline for professionals and support the IWF's hotline tackling CSE/A. Collectively the partnership delivers the annual UK Safer Internet Day (UKSID) each February. Safer Internet Day reaches nearly half of UK children and over a quarter of parents, with online safety messages and tools that make a real difference: in 2019, 60% of parents had a conversation about online safety with their child as a result of finding out about Safer Internet Day.

Our programme of work is currently funded by the EU with funding agreed until the end of 2020. On leaving the EU, there will be a substantial funding gap for the three organisations of around £1m per annum, without which this crucial online safety delivery could cease to happen. The Government needs to ensure there is financial support for this education work, and that the work of the regulator fits within the range of organisations and initiatives already working within this area.

Support for education: Education in this space is key to support regulation and ensure that people everywhere know their rights online - and their responsibilities where they have them. It will inform people's expectations and understanding of this system, but to go beyond, as the range of issues that are priority issues for young people, go far beyond the issues outlined in the white paper. UKSIC already delivers a range of educational activities in formal and informal educational settings, and these need regular review and updating in response to rapidly changing tech and new and emerging harms. The importance of education in this space requires engagement, joint working and commitment between relevant Government departments to ensure educational settings are equipped with the capacity and skills to be able to support young people to stay safe online. In response to the emerging trend for self-generated CSE/A imagery of 11-13 year olds, we need better sex and relationship education, and in particular to educate young girls in the 11-13 age range of the dangers of self-generated sexual content and sharing that content online.

Support for awareness raising for behavioural change: There is a need for large-scale awareness campaigning on aspects of online safety. Government must be focusing on positive behavioural change in online users, in order to prevent risk and harm taking place in the first place. Education and awareness raising campaigns must focus on how to develop healthy and positive interactions online based on respect and consent. We are calling here for more and better support for awareness raising activities, for example Safer Internet Day, including financial support from the UK Government to continue this hugely valuable activity. We are also calling for a national prevent campaign and to put additional funding and resources into those who request and need help when they express concern about their activity and escalation online, before they cross the line of accessing illegal content online.

Development of new communication tools: We would welcome the creation of a labelling schema to support users, particularly parents, understanding of apps and services. Much as nutritional labelling helps people make positive choices about their own and their children's healthy eating, labelling for online apps and services would be a significant development to help people (especially parents) manage their own and their children’s online safety.

Ensuring quality and consistency: As the spotlight on online safety increases, government should take steps to ensure that education, campaigns and organisations are producing high-quality and consistent messaging for the public.

Question 18:

What, if any, role should the Regulator have in relation to education and awareness activity?

Education and awareness should focus on the skills and competencies required to navigate and benefit from technology and online services. It is our view that this should be the responsibility of Government primarily to lead and co-ordinate effective campaigns which will require input from Department for Education, Home Office, DCMS, Cabinet Office and Department for Health. We do not envisage the regulator taking a lead role on the education and awareness sector, but nevertheless it has a role to play in this space.

Role for the regulator

- Assisting in supporting the education and awareness community from the issues, trends and learnings from its work with industry and transparency data, to ensure that the best advice in relation to safety concerns and safety tools, for example, are available.
- Ensuring that it is promoting its remit and signposting to support for the public. The regulator may have a role in helping organisations, such as schools, in highlighting effective online safety organisations.
- Helping existing services to address complaints (as previously outlined) that may arise regarding incidences in schools
- The regulator could also play a supporting role in key awareness raising initiatives, such as Safer Internet Day

Education and awareness largely outside the regulator’s role

- The issues that the regulator is addressing, and the services that it is covering, is not the full experience of young people’s and other users online lives, and education has a key role to play in supporting young people around all aspects of their online lives.
- The work on online safety is fundamentally about empowerment. An awareness of risk is important, but the messages are absolutely about helping young people to manage their own online lives, so they can look after themselves, look after others and contribute to the wider community.
- The most effective online safety work that takes place in the UK takes place in schools, working with children and young people, school staff, and parents and carers. Regulators can be involved in education, as education can be a part of their work, but we do not see regulators taking the lead in these areas. Online safety education professionals are also needed to carry this work forward to children of all ages and all abilities.
- Everyone has a role to play in this space - collaboration brings the best outcomes, and we have found in our work, that financial and in-kind support from industry (in the right way) can help to invest in education work and help to disseminate and get the word out to the right audiences. We see the regulator can take part in this, but do not see it as taking the lead.
- Education is a devolved mater and therefore the regulator is only able to work to support the Department for Education, Welsh and Scottish Governments and Northern Ireland Executive.