Childnet Response to the DCMS/Home Office Online Harms White paper

30th June 2019

Person responding:

Will Gardner

CEO, Childnet; Director, UK Safer Internet Centre

will@childnet.com

0207 639 6967

About Childnet:

Childnet is a children's charity with a mission to help make the internet a great and safe place for children and young people. Since 1995 Childnet has delivered a positive impact with its empowering, youth-led, evidence-based and collaborative approach to empower children and young people to use the internet safely and positively.

From its innovative resources for 3-18s, parents, carers and teachers, to its pupil powered e-safety programmes, Childnet has stayed at the cutting edge of the latest tech trends by speaking to thousands of children and young people face-to-face each year.

As a partner in the UK Safer Internet Centre (UKSIC), Childnet coordinates Safer Internet Day, which reaches millions of UK children every year.

It achieves a wider impact through giving young people a voice and influencing best practice and policy, both in the UK and internationally, sitting on Facebook's Safety Advisory Board, Twitter's Trust and Safety Council and the Executive Board of the UK Council for Internet Safety.

For more information, visit www.childnet.com and www.saferinternet.org.uk.

Consultation:

Childnet support the aims of the online harms white paper. We see the need for and want a safer online environment for children and young people. We want industry to meet its own commitments and enforce its own rules, as well as transparency and accountability to help ensure this is taking place, and developing user trust and confidence in the tools and services available to them. We see the measures set out in the Online Harms White Paper as a significant step. The introduction of the duty of care seems to be a sensible and proportionate approach in this area, and we are supportive of the intention behind it, and will work to support its practical application.

However, we also see this step needs to be matched by an equally significant step, to ensure users have the knowledge and skills to use these services safely, to be clear about what is acceptable and what is not acceptable on these services, to know what to do to report and seek support, and have clear understanding and expectations of these processes. We want to make sure that education is not an afterthought in this area, or in the area of online safety as a whole. It is noticeable that this issue was only addressed in the last part of this document, and it is important to reflect that this positioning is not a reflection of the importance of this issue.

A consideration must be that all the focus and funding for online safety policy is not placed solely in the regulatory side of this work, as education has a core part to play, and the two are indeed complementary. The regulator will need to share important information that can inform education work (in issues and trends for example). The regulator could act as a signpost to relevant resources, information and organisations in this area. And all education work in the UK will need to inform and raise awareness about the regulator, about what it can do, as well as what is beyond its scope, to set users' expectations of it.

We would want to ensure that resources from industry that are used to fund the regulator should be additional money made available from industry, rather than diverting funds away from the vital education work they are supporting. If all available resources were diverted to the regulator, then we believe that would have a serious impact on preventative measures and education progress in this area.

Industry are recognised as important funders of education and awareness in this area, and at Childnet and as part of the UK Safer Internet Centre, we have had funding and in kind support from most major industry players to support our education and youth voice work. Careful consideration needs to be given to placing the regulator between industry and education efforts and initiatives, as there could be both advantages and disadvantages to this. Where industry and NGO partners have shared goals, a constructive partnership can be developed to achieve effective outcomes.

Transparency reporting: response to question 1

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.

Transparency and Reporting

Transparency is important, both for accountability of the service provider and for informing users and developing user trust.

The most obvious area where transparency 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.

- **Caveats to numerical transparency data:** Bringing greater transparency to the systems behind the reporting process would also be of benefit and allow the service provider to be more accountable to their users. The areas covered in 3.17 where the regulator has the power to require annual reports from companies are sensible. It is our understanding that these reports are likely to be on global rather than a national level. The approach suggested in the transparency reporting templates in the Government response to the Internet Safety Strategy Green Paper (pp67-71) will provide transparency reporting in numerical form, and there is value in this. However, it is important for there to be some customary caution in interpretation. Numbers can be useful, but there has to be a caution that there can be numbers for numbers' sake, as well as that they can also be misleading. 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 is not an effective way to draw conclusions about a service's reporting/moderation if used in isolation. AI may also be involved in the process to support the work of human reviewers.

  Online services are different, and although some data may be comparable, comparisons may sometimes be misleading due to the differing nature of the services.

  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 – what is the average length of time before making a decision. Clearly this will also differ for different types of content, video for example. We would expect to see the data around response rates available as part of transparency reporting by platforms.

- **Granularity of transparency data:** The data of such a transparency report will need to be granular, as some service providers provide very different services, and the tools and

processes used may be different for the 'Live' service to the main service for example, and this differentiation would be important for the purposes of transparency.

- **Accessibility of transparency data:** The development of transparency data is important, but the data only brings transparency if it is read and used. One can imagine that the data from transparency would be useful for informing education and awareness work, which seeks to empowers users to use online services safely and responsibly. We would encourage consideration to be given as to how the results of any transparency gathered by the regulator (3.18) will look to be shared with users, as this is a key part of developing user trust and confidence. 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. This could be combined with existing education and awareness work, but it will also need to be separate.

What more can be done

Effective reporting systems (of online service providers) are crucial for ensuring users' safety on social media, gaming and messaging services and key to this is user confidence in these processes. We strongly agree 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, include, and these could also be comprised in transparency reporting and/or part of the codes of practice to be developed by the regulator:

- **Ensuring there is no systemic failure with reporting:** There are mechanisms for testing the effectiveness and quality of processes, for example through random sampling or 'mystery shoppers'. The power to require this information should be included in the powers that the regulator has, as outlined in 3.17. It would be of benefit to know if these approaches are being employed by service providers.

- **Recognising that content review decisions are not always straightforward:** Recognising that sometimes the decisions that service providers make on reports they receive are not easy, and this may be because the decisions are not always based on the full information or context. There are challenges in the 'grey areas' in relation to providers' terms and conditions and how the line is drawn between content that is acceptable or unacceptable. A good example here is in a recent Community Standards Enforcement report from Facebook which included data from appeals. Under the heading bullying and harassment, 496K pieces of content that Facebook had removed were appealed by users. Out of this, 80.2K were restored after the appeal.

  In some cases, it is the context of a post or element of a post that makes it more clearly a breach of Terms and Conditions, for example an image that would not break terms when considered in isolation, but that would break terms when considered in combination with more information (for example, a comment or a name of a group). Clearly, reviewing reporting procedures to enable reporting systems to be more effective is key, and the opportunities for the public to provide more context and better reports is important here. Reviewing procedures could provide a better understanding, and inform how to improve systems, set expectations on good industry practice and clarify the public's expectations and lead to better reporting. Allowing for an appeals process is another way to enable to provision of greater context. We asked our Digital Leaders what they would do if content that they had reported was not taken down, and the response was overwhelmingly to report it again to the service provider. In this way we see that making better mechanisms for repeat reporting would be of value to users, with ideally the opportunity to provide more context.

- **Future-proofing reporting**: Reporting functions need to be adapted, improved and tested for emerging trends such as livestreaming and virtual reality. This should be clearly communicated to users when these new technologies or functionalities are launched. There are areas we would expect a regulator to be looking to review to see how the reporting system and management of harmful content/conduct on a platform can be improved. Areas the regulator can explore include:
    - **Blocking of sharing of content that has already been deemed harmful:** can content that is known to have broken the terms and conditions and been taken down, be recorded in some way, so it cannot be re-posted/uploaded? Can this happen across platforms? Steps have been taken with Non-Consensual Image Sharing, but can this be widened to cover other areas too. It needs to be explored whether hash list technology can be applied to other imagery which has been deemed to break terms and conditions of a service, for example nude/ nearly nude images of children/teens, pornography, violent content, violent extremism, bullying content. This could help prevent the re-posting of such content that has already been deemed to break the Terms and Conditions of a service. This in turn has great potential value, for example in preventing re-victimisation. In addition, the knowledge that content can reappear could be a disincentive to reporting content in the first place, and steps taken to address this would have great potential benefit. If the prevention of re-posting of content that breaks Terms and Conditions can be achieved by a service provider, can this be shared with other service providers, so the content cannot reappear on another service, following the intent behind the regulator fostering greater levels of cooperation between platforms in relation to online harms (3.25).
    - **Transparency about other measures:** there are a range of measures that service providers can take in order to improve safety on their service. In some cases there may be a compelling reason not to make these measures public to users (thinking about the potential gaming of the system by those seeking to test the rules, for instance), but alternatively there may be measures where this is not the case, and transparency would be helpful. The regulator can provide a useful function here, in knowing the steps that companies are taking, and in establishing whether companies are fulfilling the duty of care.

      We do however see real potential for tools for transparency being developed and put into the hands of users. The SWGfL have developed a 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. This has the potential to be expanded to cover other IWF services, such as the hashlist, or searchlist, and could enable users to know which services provided by the IWF are being taken up by their members. We see this tool as having the potential to really empower users to know what steps the services (wifi provider in this case) are taking, or rather if they are taking all available steps, and we believe in the potential for this model as it can have a wider application, even for testing if parental controls are applied.
- **Education around terms and conditions and the reporting process**: there is the need to encourage 'better communication between industry and consumers, including on guidelines and terms and conditions' (Internet Safety Strategy). Research supports the need for this communication and education, as young people do not always know what breaks the rules and should be reported, or are unclear about the anonymity of reporting. In our research as part of Project deSHAME, in relation to online sexual harassment among young people, the top reasons for not reporting to social media were 'I don't think it would help' (43%), 'I don't think they would do anything' (40%), 'I would be worried that the people involved would find out or get notified that I reported them' (33%), 'I don't know how to' (18%), 'It's too much effort' (18%).

This issue is relevant to reporting to others too, to teachers, police and parents, where young people are dis-incentivised to tell because they are not clear on what will happen as a result, and getting into trouble, or being found out to have 'told', is a relevant concern. Education around the anonymity of the reporting system is an important addition here. More has been done to make clear that reporting is anonymous on services, for example on Instagram they make this clear on both the process to making a report, as well as on the feedback you receive.

- **Education around expectations and duty of services:** users need to know what is going to break the terms of the service they are using, both so they don't inadvertently break the rules, but also so they know when the threshold has been broken. Services and platforms should have clear and prominent Terms and Conditions for use of the service, as well as numerous timely moments used to reinforce this to users while on the platform. Young people have consistently said that they either do not read Terms of Use or Terms & Conditions or they find them incomprehensible. Steps should be taken to make these terms accessible to all users. One in five young people aged 8-17 also reported that if it was a service that they really wanted to be on, they would always accept the terms and conditions (Our Internet, Our Choice, 2019, UK Safer Internet Centre). This emphasises the need for ongoing digestible communication and awareness raising activities from services to remind them of key aspects of what the standards of the platform are.

'Super complaints': response to questions 2 and 2a

2. ***Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances? Question - yes***

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

The new initiative, the Reporting Harmful Content (RHC) platform, (https://reportharmfulcontent.com/) part of the UK Safer Internet Centre, can play an important part here. It is to support users facing legal but harmful content online. The RHC are providing a service where users who have already made a report to service providers, and are not happy with the outcome of their report, can contact them. It is derived from the model that the Professionals Online Safety Helpline (POSH) provides for professionals working with children, which escalates 10% of the reports they receive and have a 95% success rate for any content they escalate to industry. The Report Harmful Content hub launched six months ago, in December 2018, and since then 87% of the cases it has escalated to industry providers has led to the removal of the harmful content in question.

If the regulator does not see itself in the position to take individual complaints, then the RHC platform is ideally placed to work in collaboration, if provided adequate funding. It will also have an insight like no other organisation to the parts of the reporting system on specific services which are not functioning as well as they should. Aside from that, it is not clear who the designated bodies could be. Could it be local bodies, such as schools for example, or national services such as Childline and CEOP, or could it be more open to local level, for example schools? **Clarity about who can report to the regulator, and under what circumstances is a crucial part of public confidence in the new regulatory system.**

Other complaint measures for users: response to question 3

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:** Many users find that across different platforms, the categories that they must submit reports to are unclear or too specific and may not cover what they want to report. This may include reporting where they are not reporting the actual content, but that they are worried about a friend or another user, or perhaps when the report is not covered by the categories that are presented by the platform. More education needs to be done about reporting across the different platforms as users are using multiple platforms (often simultaneously) that have a variety of different functionalities. For example reporting live streaming as opposed to reporting permanent content. Government should encourage consistency 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. If members of the public have a particular concern about how a report has been dealt with, or a breach of duty of care, there needs to be clarity on what the regulatory system can do to support 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. At present the Professionals Online Safety Helpline provides this service for the children's workforce, and the Reporting Harmful Content Platform provides this for the public as a whole. Other countries provide this service to their citizens, including children and young people, such as the Office of the e-safety commissioner in Australia, and NetSafe in New Zealand.

  For those users who wish to raise concerns about specific pieces of harmful content or activity, in addition to continuing to promote reporting to service providers as well as to key relevant agencies, such as CEOP for suspected grooming, the Government should also assist in promoting the Reporting Harmful Content platform (RHC), referred to in the answer to question 2. The RHC provides a clear guide to reporting on popular platforms, and for those who have made a report to the service provider but are not satisfied with the outcome, reaching out to the RHC can result in getting content taken down immediately. This service is a valuable addition and has clear advantages where the harmful content is appearing on more than one platform, so a response by a single social media provider can only provide a part of the solution – RHC and POSH can address all the platforms on which that content appears. The POSH helpline also provides the same invaluable service to professionals that work with children (who are often the frontline of online safety issues and in need of such

support). The challenge with any such service is in making sure that people know about it, and this is where the Government can have a key role to play. There is a clear need for these two services, and they are unique and potentially key for the regulator and its effective functioning. They do however, need both financial support, as well as support to help ensure that everyone that needs this service knows about them.

Childnet's Digital Leaders were asked what they would do if something they reported was not removed and why. Most felt they would report it again to the industry providers. An improvement in the system here would be helpful and empowering to the user. We are seeing the beginnings of an appeal process starting, for Facebook, for example, for those that have content taken down and are not happy with this decision. We would like to see better systems in place for those who want content taken down, and the Reporting Harmful Content model provides a great example of what could work outside the service, but also we should look at what providers can provide on their service itself.

- **Enabling reporting for non-account holders:** The Codes of practice will outline the requirement for reporting functions to clear prominent and accessible to users. A relevant addition is to ensure it is easy for people to report content with service providers without being a member of a service/having an account. These were outlined in the Codes in the Government response to the Internet Safety Strategy Green Paper.

- **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. Those who may have had their content removed, or accounts suspended must have clarity on why this has happened in a clear and accessible way (without identifying the reporter) and signpost them to further support. They should also have an option to appeal if repeated reporting has been a method of trolling, cyberbullying or discrimination. 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, our work in Project deSHAME showed that young people with SEN were engaging in harassing behaviour but not supported or fully cognisant of the impact of their behaviour. Taking down their content or suspending their account will not change their behaviour but potentially isolate them even further.

Education and awareness on harmful content and how to report

- **Education about what to report:** Many users are viewing or experiencing harmful content but are not reporting. Improving industry reporting is important, but it will need to be alongside education and awareness – ie improving people's awareness and willingness to report in general. In some cases, unhealthy norms have been established and awareness on when the line has been crossed in relation to 'acceptability' must be raised, which indicates a wider educational need around themes such as inclusion, healthy relationships, social pressures and critical thinking online. This goes along with 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:** Users need to have confidence in the reporting system, so that they can be sure they won't get into trouble by using it. Education and awareness can help to address any potential barriers to using reporting. They need to

understand, for example, that when they report, their anonymity is protected. Education on how best to report, such as providing as much information, context and specifics will help moderators understand the full context and come to quicker and more accurate decisions. In our Project deSHAME, focussed on tackling online sexual harassment among children, barriers to reporting were found in relation to reporting to social media, as well as to law enforcement, parents, teachers and so on, and identifying these barriers, and taking steps to overcome these, are crucial, and will have an online and an offline component.

- **Support reporting offline:** We also need to make sure users know where else they can report (not just for themselves, but for their friends too, for example) and get help. The online part of harmful content is important, but in instances like sexual harassment and cyberbullying the user may have a clear need for offline support. There are also offline implications of reports that are made to service providers. This can be for things which break Ts&Cs and which are then taken down, but also for things that don't - or are not deemed to - break terms. Where reporting is a call for help, 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 should be key elements of any reporting journey.

  There is also a focus that can be provided to support reporting offline. This includes developing the capability of front-line workers, such as professionals working with children, including front line police support, and school staff, and also parents and carers. These in turn may wish to report to service providers in conjunction with children in their care, but they also need to capability to manage (including knowing when, how to and where to escalate for example) reports and disclosures themselves. Our UKSIC partners, the SWGfL, include in their response, the 'appropriate levels of training for all members of the police about the whole array of online crimes and how these might be presented by a victim or on victims' behalf is essential in order to improve the response that victims of internet crimes receive'. In our work on online sexual harassment among children, focussing on addressing the under–reporting of this issue, a key focus is on educators and law enforcement to both promote the avenues to reporting, as well as being ready to respond to such reports.

- **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.

The role of Parliament: response to questions 4

4. ***What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?***

We agree with the suggestion that the Regulator should be independent, though subject to Parliamentary oversight, and with the regulator making regular reports. 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 and the regulator must remain politically independent.

The codes of practice need to be practical, based on evidence 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.

Scope: response to question 5

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

It is important, and outlined in the White paper, that 'the regulator will ensure clarity about what the regulatory regime means in practice for different company's' (4.5). Clearly services are different. And also some areas of online harms are more challenging to manage than others, and clarity is key here to effective industry action and compliance. The balance inherent in this that needs to be struck is to ensure that users' expectations from the services that they use are uniform and accurate.

- **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. This may be beyond the scope of this White Paper, but it is a key issue that needs addressing.

  With the growth in popularity of such services, like WhatsApp, there is going to be a natural expectation from the public that the regulator will be able to cover such services. After all, these services do fit the definition of enabling users to share user generated content and interact with each other. The concern of the public will be with the online harm that they see, not so much on what service it arrived by. Ultimately it may well be on the same device, for example a mobile phone, that they experience this harm. Young people's needs extend to these services too. As such, we welcome that alongside this White Paper there is consulting on what regulatory requirements can and should apply to private communication services p50, though we are not aware of this work and how it is being carried out. It is

important to hear more about this work, as it is directly relevant to the work of this White Paper.

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. There is a secondary risk that relates to the challenges in making clear to end-users the remit of the regulatory regime, what is in scope and what is not.

- **Gaming:** We would recommend that online gaming is 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.

  In the survey (June 2019) we put to our Childnet Digital Leaders, one young person responded:

  "I think that many young people feel that they know more about Social Media and gaming than adults. I would say that chat rooms on games aren't covered too much, and thus is left as a minefield for younger people, who can be affected by the content and opinions posted there."

Private channels and private communications: response to questions 6, 7 and 7a

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

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).

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.

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

Defining private communications is challenging, as end-to-end encrypted (E2E) services can have group functions, with large numbers of members. Although the technology could be defined as private communication, as the communication is not accessible to anyone outside the intended recipient(s) as well as the company providing the service, there could be a large number of people part of the group and so receiving the message. 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. In the converse, Instagram Stories can be used by users to target only specific contacts and can therefore be seen as more 'private'.

We are aware that a range of new technology can be used for malicious purposes. For example, unsuspecting members of the public receiving 'dick picks by Airdrop'. People subjected to such behaviour need to be able to report this form of sexual harassment, and if this falls outside of the scope of this White Paper, it needs to be clear where the responsibility for this does lie.

People are going to be motivated to report things that are harmful or potentially harmful that they see in their or their children's use of technology. There is a risk of public confusion with some services being out of scope. There are real problems with the same piece of content conceivably being able to be reported for one service, but not another, and there are risks that this can undermine the proposed regulatory regime. Similarly the same problems exist if lines are not only drawn between services, but within services – ie. if a group on a private network has above a certain number of members.

7a: What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

All the same options should be looked at to assist user protection on private channels. Clear, prominent, accessible reporting functions, as well as other safety tools should be available. For the reporting, on E2E services, reporting should automatically (very easily) share with the service provider a screen grab or the message trail, to allow for effective review. These services should be included in having transparency requirements, and they should need to demonstrate to the regulator what they are doing to keep their users safe.

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, and see the discussion around safety vs privacy needs to be fully explored and explained. What measures that are used by other services, which would form part of their duty of care, can be applied for such private services, and the rationale for their application or non-application, should be clear. For example, the use of the hash list of CAI to prevent the uploading or sharing of known illegal content – can this be applied prior to the encrypting process to prevent end-to-end encrypted services being used for the distribution of CAI or not, and why?

Ensuring the regulator acts in a targeted and proportionate way: response to question 8

8. ***What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?***

We welcome the clear mention of the rights-based approach in 5.12 and the obligation to support innovation 5.11.

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, ranging from large companies, to small companies, social enterprise and charities. The regulator should be available to provide advice and guidance, and look at ways to disseminate this advice and this service widely.

Childnet see that there would be advantages in enabling collaborative working between industry and the regulator, as issues can sometimes arise very suddenly and carry great potential harm. This essence is captured in the Christchurch Call, highlighting the urgent need for action and cooperation among the wide range of sectors, 'including governments, civil society and online service providers, such a social media companies, to eliminate terrorist and violent extremist content', and we would include regulators in this.

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) when emerging new threats or issues arise which are in the public interest. For example, 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. The regulator should ensure that all measures and responses are proportionate by consulting with experts who have grassroots involvement with users and with industry.

The advice and support from the regulator to help start-ups and SMEs comply: response to question 9

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

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, ranging from large companies, to small companies, social enterprise and charities.

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 development of self-assessment tools could be a useful addition here. Our partners in the UK Safer Internet Centre, the SWGfL, have been very successful in developing such tools for schools, with the result that over half of schools in this country use 360 Safe.

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.

The regulator as a new public body or an existing public body: response to questions 10 and 10a

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

There are advantages either way, and it is difficult to pass a judgement, particularly without seeing a clearer proposal for the existing body/ies or for a new one.

A practical suggestion would be to on an initial basis house this at an existing regulator for a pilot period before a review, and a final decision is taken. Whatever decision is taken, it will need to work closely with existing organisations, like the IWF, where the public can report illegal online images, as well as the Reporting Harmful Content hub, where users can report harmful content.

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

We have no strong opinion, but would be open to the suggestion of Ofcom, as it is an experienced communications regulator, with an already broad remit, and it is known to the public.

Industry funding for the new or existing regulator: response to question 11

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

We have no feedback on the basis of industry funding. 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. At Childnet, we have received funding from industry for a range of education and awareness work, and even where, with EU-funding we organise big national campaigns such as Safer Internet Day, or respond to key new issues affecting children (such as Project deSHAME tackling online sexual harassment among children) we receive part-funding from the EU, and need to raise the rest, with industry being a key potential contributor. Safer Internet Day in the UK is the

biggest national online safety awareness campaign in the world, and it is growing each year. It received 50% funding from the EU, and industry contributions either financial or in-kind are vital. Last time around Safer Internet Day reached almost half of 8-17 years old in the UK in 2019, and over a quarter of parents with online safety messages. The concern we have is to ensure that industry recognise and are able to meet this need, whilst also meeting any requirements to support the regulator.

The IWF are a key UK body, and a global leader in the fight against CAI. Consideration of any requirements on industry to fund the regulator should also be given to ensuring the IWF can continue in its vital role.

Increasing the amount of industry contribution to the area of supporting online safety could be one answer. The concern has to be though that the establishment of a regulator can impact on what financial support if available for the crucial education and development of skills work with children and young people and those that support them, across the whole range of online risks and harms, necessarily broader than those risks and harms that fall within the remit of the regulator. We asked our Digital Leaders about the areas that they see are priority areas in this area of discussion, and they included many of the online harms outlines in the White Paper, such as grooming and cyberbullying, but also included other issues, such as peer pressure, mental health, and body image. It is vital that those organisations that are working directly with children and young people are funded to work on those issues.

In the survey (June 2019) we put to our Childnet Digital Leaders, one young person responded:

'I think that we are never taught enough about how to manage our Digital well-being. As many people are aware, the internet can and has had negative effects on young people and their mental well-being. We are often never taught about how to keep ourselves happy on the internet and we are only ever taught about how to keep ourselves safe".

The sanction powers available to the regulator: response to question 12

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?***

It is right to be exploring all options, and looking at existing precedent in other sectors. For example, there is useful precedent in the risk-based approach in money-laundering regulation and more broadly the financial services regulation.

Opportunities for innovation and safety technology by UK companies: response to question 15

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?***

The technological arena is a fast moving one, and the Government is right to look at Safety by Design, to ensure the adoption of safety measures are considered and implemented at the outset of new technologies, rather than after they are developed, and even become successful and popular. The challenge to overcome here is to enable this and not to hinder the development of new technological services; rather it should look to encourage the development of safer online services, and the government may have a key role to play here.

Childnet want to see all online providers using all the technologies available to identify and prevent illegal and harmful content (images and video) to be uploaded, specifically the use of the IWF hash list.

Continuing momentum is important in this area. 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.

Support for safety by design: response to questions 16

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

Historically, popular services have often become popular before the safety tools and processes are firmly established, and as such, 'Safety by design' is an important aim and initiative. However, one of the challenges, in practical terms, is that safety often costs funding that a level of success/popularity will enable. So the forces of the market can lean towards safety second, and work is need to redress this, and we see an opportunity for government here.

Clearly making safety a marketable asset is important in the response here, as safety can help bring success in this way. It could be making available support, both technical and financial, for start-ups grappling with this. It is important that any measures that the regulator takes also take into account organisations and companies which are not major social media companies, as this has been much of the focus up to now.

Government support for people's online safety: response to question 17

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

A holistic approach

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. As discussed in our response to the UNCRC General Comment on digital rights, states must recognise the importance of the access to, and use of, digital media and their potential to promote children's rights such as their right to freedom of expression, access to appropriate information, participation, education, leisure, play, cultural life and the arts. They must also ensure that there is equal and safe access to the digital world for all children, including those who may be marginalised in society due to other forms of intersecting inequalities.

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).

It is essential that government take a holistic approach to keeping children safe and happy online.

Education is key

Education needs at least to match the regulation, to 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. Young people will need to talk to parents, carers, friends, teachers, law enforcement and wider to support them with these issues. Just as there are advantages in transparency in the reporting process to industry providers, young people would benefit from knowing what would happen if they report elsewhere, such as to a teacher.

One Digital Leader told us, when answering 'What do you think is an issue which should be covered more but isn't really covered now (for e.g. in schools):

"What the outcomes of telling teachers or trusted adults about your problems are."

Our work in Project deSHAME looking at online sexual harassment amongst young people shows that many young people are already using tools on services and platforms such as blocking or reporting, but are less likely to tell adults (schools, police, parents/carers). This means that the impact of what they have seen or experienced may not have been dealt with, even if they have reported to the platform. It also means that young people are feeling like that they must deal with harmful or

upsetting content on their own, without support or advice from offline means. This needs to be addressed, and education as well as training and empowering those working with children is key.

Positive behavioural change

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. This year for Safer Internet Day, we focused on the issue of consent in a digital world and found that young people lacked the practical strategies needed to apply consent online. After the Safer Internet Day (SID) campaign, of the 45% of 8-17 year olds that heard SID messages, 84% said they were more aware of the importance of asking for permission before sharing content about other people.

Financial support

The Government needs to ensure there is financial support for this education work. For the development of skills in children and young people, for the awareness raising and education with parents and carers, for the training of professionals working with children. There has been a lot of work done in this area in the UK, and the Government needs to ensure that the regulator fits within this system. Educators must also have clarity on the role of the regulator and continue to empower children and young people to be safe and responsible digital citizens. Awareness campaigns, such as Safer Internet Day, draw on a huge national collaboration and achieve huge dissemination of messages, and reach and impact with the target audiences, and more support can make this day bigger.

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. This is to ensure that users are receiving accurate, relevant and factual information, and receiving it in the right way.

Role of the regulator to education and awareness activity: response to question 18

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

We see the potential for the regulator to add value in several ways, and support education and awareness:

- The regulator can inform the education and awareness community with issues and trends that are coming to its attention.
- The regulator can assist in supporting the education and awareness community from the 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.
- The regulator should ensure that it is promoting the role that it is doing as well as ensure clarity on its remit and make sure that others are supporting this area of work. The regulator

can also effectively signpost people to the right organisations and sources of information and support.

- The regulator could also play a supporting role in key awareness raising initiatives, such as Safer Internet Day. Last year over 2000 organisations got involved and supported the Day, and we would expect to see the Regulator playing its part here too.

We do not envisage the regulator taking a lead role on the education and awareness sector, and this is for a few differing reasons:

- 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. The harms outlined in the White Paper are important and demand the attention they are having, However, there are further risks online facing children and young people that are not covered, many of which have a strongly social element. Peer pressure, self-esteem, body image, healthy relationships and friendships in an age of technology, as well as impersonation and hacking. We asked our Digital Leaders what areas they think should be covered more (for example in schools), and many issues, and many of the online harms listed in the White Paper were included in their responses, such as grooming, cyberbullying, pornography and violent content and sexting. Also included were other areas, such as privacy, educating parents, how to manage wellbeing, protecting your online reputation, plagiarism and copyright, peer pressure, age restrictions, managing time spent on social media/devices as well as learning about the benefits of social media.
- 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. Digital citizenship in essence. Knowing what to do when things go wrong is part of this, as are key preventative messages.
- 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 (including those with Special Educational Needs), parents and carers and to school staff and other professional working with children. For example, the development of online safety resources for schools to use.
- There is already a lot of work taking place across the UK. In fact, the UK is seen as something of a world leader in this area. New initiatives and activity need to recognise this at the start, and what is needed is perhaps less another organisation providing education, but strong and consistent support for work that is already taking place in this area, for example the support of Safer Internet Day in February each year.
- Everyone has a role to play in this space, schools, parents, government, charities, regulators and even industry. 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.
- Devolved nature of education, means that work in this area requires supporting the Department for Education, Welsh and Scottish Governments and the Northern Ireland Executive.