Childnet Response to the DCMS Internet Safety Strategy Green Paper

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 one of three charities 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 Child Internet Safety.

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

Childnet response to **Chapter 3** 'Introduction'

Childnet agree with the three principles underpinning the Strategy:

- *What is unacceptable offline should be unacceptable online*.
- Our remit extends to children and young people and those that support them, but we agree that *all users should be empowered to manage online risks and stay safe*.
- and also that *technology companies have a responsibility to their users*.

As partners in the UK Safer Internet Centre, **we share the Government's aim of *making Britain the safest place in the world to be online***. We welcome the support and recognition of the work of Childnet and the three partners of the UK Safer Internet Centre throughout the Internet Safety Strategy.

Childnet support the view outlined that, due to the global nature of the technology, we need to work with other partners around the world and international institutions. The same issues are affecting children across the world, and we need to share good practice and learn from the policy and educational responses happening globally, as well as look to work in partnership.

Childnet have a strong track record here; even as far back as 1998 we worked to connect hotlines across Europe, establishing the INHOPE Forum which went on to become the INHOPE Association. In our role as one of three charities in the UKSIC we are part of the INSAFE network of European Safer Internet Centres, continuously sharing and learning from each other. We have just published an important research report (as part of Project deSHAME) looking into online sexual harassment among children, working together with NGOs in Hungary and Denmark, and the findings were more similar than not between the experiences of young people in these three countries. Recently Childnet was invited to share its work at a conference organised in Sydney by the Office of the eSafety Commissioner in Australia and NetSafe in New Zealand. We have worked collaboratively with NGOs, as well as with governments globally, and also industry, and we are members of both Facebook's Safety Advisory Board and Twitter's Trust and Safety Council.

Childnet response to **Chapter 4** 'Our strategic response'

Background

Childnet have been active participants in UKCCIS since its inception, and were also active members of the preceding Home Office Taskforce on Child Protection on the Internet since that began in 2001. We are strong supporters of the view that everyone has a role to play in keeping children and young people safe online, and UKCCIS, and the Taskforce preceding this are embodiments of that response – all sectors working together to help keep children safe online.

Childnet's response

The Strategy outline a number of changes to UKCCIS, and we will respond to these in turn:

Childnet response 4.1

"The Council will consider all users, not just children, and change its name to the UK Council for Internet Safety (UKCIS)" (pg11)

- **We do not support the proposed change of UKCCIS to UKCIS**. In fact we are concerned at the impact that such a change could have on the issue of child safety online. Our concerns about broadening out the remit relate to:
    a) the effectiveness of the body, which we believe would be weakened by broadening priorities and focus

b) the different personnel needed, which together at the same time as slimming down the Board risks less informed discussions rather than more. For example, the UKCCIS Evidence group would need completely different personnel to include adults in their remit.
c) Children have unique needs. Children are pioneering in their use of technology and are by definition vulnerable.
d) Rather than moving UKCCIS in a direction away from a focus on children, we would support taking it closer to children, and looking for ways in which their voice and participation can be included in discussions.

- **We recommend** a **separate body that focuses on the needs of adults, with separate working groups, and encourage information sharing between this body and UKCCIS**. There are some topics for discussion where there is overlap, such as critical thinking/social media literacy, online sexual harassment and online hate, but the response to these issues is not the same.

Childnet response 4.2

"A smaller, higher-profile executive board to set the Council's strategic direction and annual priorities" (pg11)

- We **support setting annual priorities for UKCCIS** and this echoes the original establishment of UKCCIS, whose work agenda was set by the recommendations of the Byron Review. The Working Groups were formed and then tasked with particular recommendations, and then reported on their progress to the Executive Board. Clearly the Board will need to have the ability to be responsive, as issues can arise in this area very quickly, but setting a clear work plan/priorities will make UKCCIS more effective, and give it a clearer function. There is a need to consider who would set these priorities. Some of the priorities from the Byron review are still relevant today, for example including online safety in teacher training, but there is scope anew for a fresh look, and potentially an independent expert or panel to review and make recommendations.
- Creating a smaller, higher profile Board: we would support such a step, but would **want to see the existing permanent members remain on the Board, namely the police in the form of CEOP or NPCC, the IWF, the UK Safer Internet Centre (UKSIC), and representatives of the devolved nations**.

Childnet response 4.3

"Reconsidering the role which the working groups undertake to ensure that we have flexibility to quickly respond to new issues. The important roles undertaken by the Education and Technical Working Groups will continue and we propose to expand the work of the Evidence Working Group to include adults" (pg11)

The review mentioned three of the existing UKCCIS Working Groups – **Education, Technology and Evidence. We attend all of these and would recommend the continuation of these groups**. The Education group has been prolific in producing important documents, including the Guidance for schools and colleges on responding to sexting, the guidance on tackling race and faith bullying in conjunction with the Anti-Bullying Alliance as examples. The Evidence group is a key element to championing evidence-based interventions and supporting the wider work of UKCCIS, as well as the wider UK, and we are proud to host the research highlights on the UK Safer Internet Centre website. The Technology working group has only recently started, but provides a useful element to review new products and services.

Childnet response 4.4

> *"we may decide to have an independent panel or working group which could support the government with arrangements for the social media levy" (p11)*

Depending on the outcome of the consultation, we see the value in creating an independent panel or working group to support the Government with arrangements for the social media levy. We **support a levy in principle**, as there is and will continue to be a clear need for funding to support education and public awareness. This will be particularly important, given the UK Safer Internet Centre is currently funded by the European Union until December 2018 and after this time there is uncertainty about the UK's access to this funding stream.

Initially the voluntary nature of the levy makes sense, with the option to review other options if it is not functioning. It is worth noting that the industry are already active in this space, and care must be taken for the levy not to impinge on current initiatives, including membership of IWF for example.

Conversely, as explained there is potential for the UKSIC to be ineligible to access the current EU funding streams, which means the UKSIC will need to secure £2 million per year from January 2019 to maintain its extraordinary reach and impact right across the UK, and more if we are more ambitious in our targets. **If there is a levy, we hope that is could support the UKSIC to meet any deficit from the potential withdrawal of EC funding after December 2018**.

Childnet response 4.5

> *"UKCCIS undertake a review of available online safety information and identifying gaps in resources" (p11)*

A review is proposed to be carried out by UKCCIS of available online safety information and identifying gaps in resources. As part of the UK Safer Internet Centre, Childnet has created several resources, and they have had great reach for example, the Education resources we produced for Safer Internet Day 2017 were downloaded over 500,000 times. **We would recommend that the review also take into account resources that are in the process of being produced**. We have also developed resources with EU support in conjunction with support from the Government Equalities Office, and we are also committed to developing several over the next 12 months (as part of our grant agreement with the EU). These cover gaps that we have identified already, including extending our work to support children with Special Educational needs, support for Early Years and parents and

teachers of Early years, extending our PSHE toolkit to cover online pornography, body image and healthy relationships. **Any review will need to take into account age of audience and issue**.

Childnet response to **Chapter 5** 'Working with industry to make online environments safer for all users'

Background

Childnet has been involved in all of the self-regulatory good practice documents that have been created: originally on the Home Office Task force on child internet safety which had good practice guidance covering Chat, Instant Messaging and web-based services, Search, Moderation, Social Networking Services, and in addition the two Codes agreed by the Mobile Operators, on Self-regulation on new forms of content on mobiles and Location based services. These Codes and good practice documents have had an international impact, and Childnet were also involved at EU level on the European Framework for safer mobile use by younger teenagers and children, the Social Networking Principles, and then the ICT Coalition. With UKCCIS, we have fed into the ISP Code (leading to Active Choice) and most recently the 'Child Safety Online: a practical guide for providers of social media and interactive services' with the UK Council for Child Internet Safety.

We believe this work has played a part in improving industry, and we have regularly shared these documents, such as the Home Office or UKCCIS social media providers good practice document to enquiring start-ups looking to do the right thing. And we have seen, perhaps more often, the more mature industry organisation make improvements in their provision around safety, with the main providers providing the key safety tools, including blocking, reporting and privacy settings, and safety centres for example. Self-regulation can work, but where it fails then we recognise that we need to look at other solutions. We support the voluntary nature of the Government's Strategy, but with the shared realisation that if after a period of time this does not have the desired outcomes, then other approaches should be considered.

We also believe that steps can be taken outside of 'industry'. For example, the IWF image hash list is currently available to online service providers (including hosting providers and social media services, for example). Wider take-up of the hash list (for instance by hardware manufacturers) could improve the protection of children and internet users. In addition, it could be further explored whether there are other uses for this technology in different sectors and industries. Large corporations or public sector bodies could – for instance – use the technology to protect their employees and ensure their networks are not being used for the storage and distribution of known child sexual abuse imagery.

Childnet response 5.1 Social media code of practice

"Work with industry to secure a more coherent, joined-up approach to online safety across the range of major platforms. A key part of this will be issuing the voluntary code of practice" (p15)

We support the goal of the social media code of practice, outlining agreed safety standards that can drive up standards in relation to online safety, and make an equal (but also open) market place, and

they can also help to raise and help communicate to users what their expectations should be in relation to particular services. Consistency would be helpful here as well as clear labelling, to better inform the end users.

The effectiveness of Codes rely on monitoring and evaluation, which will need to include an action if a signee has not met their commitments. This needs to be part of an effective Code.

In the review process for this Code, items outlined in previous Codes will need to be included, such as clear prominent safety information and advice for users and clear prominent and accessible safety tools.

One young person responding to our consultation into this strategy welcomed steps industry take:

> *"The social media companies add icons such as Reporting, Blocking and Privacy these are helpful because if you are in the situation of cyber bullying these icons are really useful. Also they provide very important messages which are useful, such as how to report someone and how to block someone."*

In particular, Childnet propose the inclusion of the following items, most of which were raised by young people responding to the original Government consultation late March 2017:

- Providers to ensure that **privacy is default on for new users**, enabling users to change their settings once they're using the service. This way, all users will be aware of the environment they are operating in, making a conscious decision to become more public. In the absence of effective age verification for over 13s, this privacy by default should not just be for under 18s, but it should be for all users.
- We would also want **all providers to be members of the IWF AND** take, or work towards taking, the IWF lists, including the hash list, being able to use Photo DNA or equivalent, URL list and keywords.
- Industry providers to **provide feedback to users** of the outcome of their report, and signposting to places they can go for further help. User confidence is key for reporting to work, and this transparency is essential here.
- All services should ask the age of their users and make clear the **age requirement** for their service. This is currently not the case on many popular apps, including Instagram, Snapchat and Twitter for example.
- Internet service providers typically have **Terms and Conditions** and **Community Standards** which set out the behaviours that are acceptable on the platform. There are a number of best practices that should be implemented by all services, for example 1) **Easy to understand and child-friendly**; 2) **Prominent on the site and communicated regularly to users**; 3) **Easy to report all of the listed prohibited content and behaviours**.
- There should be a process in existence for the improvement of the service provided, from a safety perspective.

Childnet response 5.2 Transparency

> *"…the possibility of working with industry to produce an annual internet safety transparency report. This could include common metrics which would enable benchmarking of reporting mechanisms"*

The Strategy talks about reporting in relation to the **Code of Practice,** and also in relation to **Transparency,** and we will respond in detail here on this issue, covering **the current evidence, the current provision** and **Gaps/Solutions.**

The evidence base:

There is no public data on the actual number of user reports processed by service providers.

- The consultation proposes a transparency report including performance metrics on take-down. Numbers can be useful, but there has to be a caution 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. Comparing the number of reports to the number of takedowns, also is not able on its own to conclude a service's reporting/moderation is ineffective. AI may also be involved in the process to support the work of human reviewers.

- There are instances where reports are not satisfactorily handled by social networks or where the issue is too complex or nuanced for traditional reporting tools to work. Currently the Professionals Online Safety Helpline offers mediation in these situations for members of the children's workforce. Approximately 10% of cases managed by the Helpline require escalation to social networks and of those over 95% are resolved satisfactorily with removal of content.
- Example case from the Professionals Online Safety Helpline (received 15 March 2017) – Contact regarding a survivor of childhood abuse, whose abuser had used her image as his Facebook profile image. He is no longer able to respond to court demands to remove the image and she is desperate to have it taken down. Services including Court, Probation Service and the client have repeatedly reported to Facebook to no avail. The profile was eventually removed at the request of the Helpline within two hours of initial escalation to Facebook.
- While many children and young people are using the reporting tools of online service providers, many do not have confidence in the reporting process, are unclear about anonymity of reporting, lack knowledge about how to report and what content can be reported.
- From our Safer Internet Day 2017 report we found:
    - Over a third (34%) of young people aged 8-17 years old said they had reported an image or video on a social media or messaging app.
    - Young people told us what would be likely to stop them from reporting an abusive image or video: 38% said 'being worried people would find out'; 33% said 'not thinking it would make a difference'; 28% said 'not knowing what to do'.
- From our research into young people's experiences of online empowerment and online hate for Safer Internet Day 2016 we found:
    - 64% of 13-15s and 71% of 16-18s knew how to report online hate to a social network.
    - Young people said they would not always know when things break the rules – 58% of 13-18s who had been exposed to online hate (which was 82%) said they wouldn't know when online hate breaks the law.
- From our Project deSHAME research into online sexual harassment among young people, we found:
    - In relation to the barriers to reporting to social media providers, 18% of 13-17s said they didn't know how to report.

Current provision:

- Most internet service providers (including social media, messaging and gaming providers) provide **reporting tools** to enable users to report.
- There are best practices provided by some services which we recommend for all providers:
    - **In-line reporting**: reporting buttons on the actual content that the user might want to report, rather than a separate contact form or email address. (For example, currently this is not provided by WhatsApp or Tumblr).
    - **Feedback:** Providing feedback to users on the outcome of a report decision (for example, see Facebook's Support Dashboard, or Twitter)
    - **Additional support:** Providing additional support and signposting to help users deal with complex issues, for example signposting to helplines or other advice. (For example, see Facebook and Instagram's suicide reporting intervention). This is also important in cases where the report has not been judged to break terms and conditions, and users need more advice about what they can do instead.
- The **Professionals Online Safety Helpline** (www.saferinternet.org.uk/helpline) provides a service for the children's workforce to provide guidance and work with industry to take down content. This includes situations where content has not been removed by industry, but the helpline can liaise with teachers and others to provide additional context to industry to enable them to remove content.
- The **Internet Watch Foundation** (www.iwf.org.uk) is the largest, most successful hotline in Europe and provides a secure and confidential place for anybody to report potentially illegal content online, namely online child sexual abuse material, non-photographic child sexual abuse material and criminally obscene adult content. The IWF is a self-regulatory organisation working closely with the online industry, law enforcement and other civil society organisations to ensure the swift removal of the illegal imagery.
- Hashing technology – such as PhotoDNA - has provided an important way of dealing with the proliferation of known child sexual abuse material online. The IWF already offers a list of known child sexual abuse images to the online industry to help prevent, detect and remove those images.

Gaps/Solutions:

Effective reporting systems (of online service providers) are crucial for ensuring users' safety on social media and messaging services and key to this is user confidence in these processes. We strongly agree with Q109, that social media platforms have a duty of care to remove and reduce inappropriate behaviour or content on their platforms. Areas for improvements we can recommend here, Q110, include:

- **Improved reporting tools:** all providers should fulfil 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, providing in-line reporting tools and offering additional signposting and advice.
- **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'. We would like to know, and transparency is important here, if these approaches are being employed by service providers. Service providers need to ensure that their moderation teams have the required skills, training and support, and that there is sufficient capacity to respond to reports in a timely manner. The Strategy talks about transparency in relation to the volume, ie numbers (Q114), of reports – this information is relevant only in conjunction with the

capacity of the teams to review these reports, ie how long is each report reviewed for. Without this information, then the numbers suggested to be gathered will not provide the insight which is needed.

- **Dealing with 'grey area' issues around Terms and Conditions:** 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. For example, this may be content that sexualises children but does not explicitly show nudity or erotic behaviour. It can also be in situations when the context 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). 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.
- **Providing a complaints procedure to users**: 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. 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. We recommend that a service like POSH (and POSH could be enabled to provide this service, either directly to the public, or to work to support other helplines working with children and parents), trusted by industry, can fulfil a similar role in the UK. This would be valuable 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, whereas POSH could address all the platforms on which that content appears. The 'Comply or Explain', where a service needs to 'comply or explain why not' is already used in this format, where there is interaction through an intermediary of the Helpline. Looking at how to make this feedback more public can be useful, taking into account the needs of the person reporting/or being reported about.
- **Future-proofing reporting**: Reporting functions need to be adapted, improved and tested for emerging trends such as livestreaming and virtual reality. 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? 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 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.
- **Education around reporting**: the strategy talks about encouraging 'better communication between industry and consumers, including on guidelines and terms and conditions'. 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%).

- **Reporting of illegal images:** We see opportunities that will arise in the future as a result of image hashing, for people to be able to report illegal images not just URLs to the IWF. For example, this could be an image that had been shared on a messaging service. We want to see these opportunities fully explored. For example, the following scenario could be a possibility:
    - Illegal image shared on messaging service (for example, WhatsApp is end to end encrypted) – for example, this could include children's self-taken images being shared non-consensually
    - Member of the public reports this image to the Internet Watch Foundation (or child reports to their school and the school reports to the IWF)
    - Image added to hash list if included in IWF's remit
    - Steps can now be taken to prevent the image from surfacing on the 'public web' before it has even been posted and potentially provide additional intelligence on offenders to law enforcement via existing channels.

  This may require legal amendments, to enable to sharing/sending of illegal content to the IWF, and has implications for content involving children between approx. 13-17 years of age around Age Verification, but we would recommend a scoping exercise to explore this.

Childnet response 5.3 Financing & industry structures

> *"We believe more needs to be done and that it is right that all companies should be involved and encouraged to play their part. This is the reason we will introduce a levy, to help us combat online harms" (p16)*

Social media levy (Q117):

As a charity, Childnet, also in its work as part of the UKSIC (which is 50% funded by the EU), looks for funding to carry out its work to fulfil its mission, and has looked for support from the EU, Government, Industry and Charitable trusts. Over the years, we have been successful in receiving support from a wide range of industry partners, including Disney, Google, Microsoft, the four big ISPs, Twitter, Facebook, Yahoo! and so on, with Facebook most recently pledging to support the scaling up of the Childnet Digital Leaders Programme by providing £500,000 over two years. Industry do play an important role by providing financial support for reaching shared objectives, as well as by providing in kind support, for example in ad credit to support the dissemination of Safer Internet Day messages.

We have looked to industry, (as well as Government, the EU, and charitable trusts) to support our charitable programmes and resource-development. This funding is key for the development of educational materials, organising Safer Internet Day, enabling youth voice and youth participation, international engagement on online safety, research, developing and running peer education programmes and more.

The idea of a levy in terms of bringing funding to support work in this area is positive, ensuring funding is available for this work. Childnet support the proposal that this levy be voluntary at the start, and in continuation if it proves effective. If not, and there is a shortage of funding in this area, then a review of how to make this a statutory levy could be considered.

Questions remain about who would be subject to this, and also who would receive this funding, as well as who would make decisions regarding the distribution (Q121). It is important that the levy is distributed according to key criteria to ensure the quality and effectiveness of the interventions supported. For example, we would recommend that the levy is distributed to charitable organisations that can demonstrate their impact, value for money and the participation of key beneficiaries (eg children) in the design and development of interventions.

Sustainability is crucial for effective education and awareness work. We have found the best support, from whichever funder, is one based on partnership - if both parties can see what is achieved by this funding, it helps when we look to make the work sustainable. It is worth pointing out that centrally allocated funding would not give this to industry. It could be that the threat of the levy could encourage more industry to participate in supporting this work, and enable such sustainable partnerships to develop.

The levy, Q119, could play an important part in enabling the continuation and the further development and impact of the UK Safer Internet Centre, which already provides a vital function right across the UK.

The reasons for suggesting the UKSIC here include:

- The provision and running of the world's leading hotline
- The provision and running of the helpline, a global first and a global leader, providing a valued system for supporting professionals working with children
- The awareness centre, which has developed Safer Internet Day into the global centre of excellence. Reaching 42% of children and 23% of parents, it provides the best opportunity in the year to effectively communicate on these issues, and engages the support of over 1600 (in 2017) organisations. Those young people that heard the SID messages, 25% spoke to someone about something or someone that upset them online.
- High quality and evidence-based educational resources
- Training for professionals,
- developing a nationwide peer education programme
- youth participation and consultation
- Research to support key initiatives, for eg on the teaching of the online element of relationship and sex education (December 2017).
- International connections, the ability to share with and learn from other key partners across the EU and across the globe.

The UK Safer Internet Centre is currently funded by the European Union until December 2018 and after this time there is uncertainty about the UK's access to this funding stream.

The UKSIC receives £1million per year from the EU (50% of the total project cost) and from January 2019 will need at least £2 million. The UK Government could use the levy to support the extraordinary reach and impact of the UKSIC post-Brexit and continue to build upon this work.

In the distribution of the levy, there are some things to consider, Q121:

- The funding should support identified priorities, ideally relevant to the industry contributing
- An evidence-base should inform these priorities, and research could also be a recipient of this funding.
- Need to avoid duplication of effort, so a level of coordination needed.
- Need to build sustainability, for which partnership is important.
- Need for evaluation of work, transparency around the funding.

Childnet response to consultation Q111 on anonymity

"Do you think companies should encourage people to use their real identity when using social media?" (Q111, p59)

This question is from the Internet Safety Strategy Consultation Questionnaire. Companies encouraging people to use their real identity when using social media, can have advantages in certain situations, but can also have a negative impact in some situations, which can of course be entirely valid, where people can participate better and feel safer when anonymous.

We carried out a youth consultation in this area, Global perspectives on online anonymity, where 86% of the respondents felt that it was important that people be allowed to be anonymous online. Despite anonymous services being perceived of as nastier by the majority, more than half said they had seen anonymity being used for positive reasons, "including for seeking help and advice about potentially embarrassing, sensitive or taboo subjects; saying compliments that you might feel embarrassed to say otherwise; for protecting privacy; for speaking your mind without being judged or facing a backlash; as well as criticising governments, corporates or speaking about controversial subjects".

Tackling those who abuse others via anonymous services, Q112 would provide a clear benefit, and it is important to find ways of providing a deterrent to such activity, but removing anonymous services is not the optimal route given the vital function they can provide.

Childnet response to 5.4 'Advertising and social media'

"The Government will explore, in an open and consultative way, how higher expectations of online safety from advertisers can be translated into a greater focus on safety from platforms" (p17)

The inclusion of advertising and social media in the Strategy is welcome, as the Literature review by the UKCCIS Evidence Group 'Children's online activities, risks and safety' Oct 2017 (p21) reveals that children dislike "there being too many online advertisements", in fact their top concern, especially among 8-11, when talking about their dislikes about social media and apps.

There is a question to answer, outlined in the strategy, about how higher expectations regarding online safety from those wishing to advertise, can translate into a greater focus on safety by platforms.

But there is a bigger question about education of users here, as well as user profiling, and its use in advertising. Education of children needs to cover an awareness of what advertising is and what it looks like online, including less obvious forms like advergames or promotions by vloggers in YouTube videos, (highlighted by the recent Ofcom media literacy report) but also about what the rules are and what to do if you think they are broken.

A discussion around profiling would be an important part of this. Profiling can support safety, as if you know a user is a child, then you can ensure no age-inappropriate advertising reaches them.

However, the provision of tailor-made advertising has also been criticised for the influence it can have on young people.

Childnet response 5.5 'General Data Protection Regulation'

Childnet support the three changes outlined specific to the protection of data:

- Privacy notices to be written in a clear, plain way that is understandable to a child user
- A strengthened right to be forgotten
- Parents will be required to give consent to information services where a child is under 13.

The latter point, addressing parental consent being required for under 13s, is an important one to develop agreed standards as to how this can be practically implemented, and enabling industry to carry out this important function. The market has not effectively solved this as yet, and the identification of good/best practice in this area would help.

Childnet response to 5.6 'Online games'

The steps outlined by the Strategy, outlining how Government will work with the **online gaming industry** are important ones. At Childnet, for example, we are actively involved in promoting awareness and understanding of Pegi age rating, parental controls and provide advice on safe gaming. We also support the identification and sharing of good practice, and exploring how the principles of the social media code can apply to interactive games.

Childnet response to Chapter 6 'How can technology improve online safety for all users'

Childnet agree with the push to 'think safety first' in the development of new technology. We have worked in this way by participating in the development of Codes and good practice, as well as providing feedback to industry on new initiatives, even, through membership of Safety Advisory Boards for example, providing feedback on proposed initiatives/products.

6.1 Supporting the internet safety technology market:

Childnet are active members of the UKCCIS Technical Working Group, chaired by Fred Langford, Deputy CEO of the IWF. In this group we are reviewing many of the newer entries into the domestic market, and we support the continuation and development of this work.

6.2 Encouraging technology firms to think safety first: (p21)

Childnet continue to promote this approach. We welcome the Secure by Default review, which will include recommendations to improve the cyber security of consumer interconnected devices and the connected services. At the Safer Internet Forum in Brussels in November 2017, a panel focussed on internet connected toys, and outlined a clear need for policy as well as education and awareness in this area.

We would support the DCMS offer to start-ups and smaller companies by producing easy to follow guidelines.

Childnet see a **role for the technology industry to support children develop their digital literacy skills**, **Q137 and 138**.

- Externally, by supporting charities to develop materials and help empower children, parents and carers and teachers (and other professionals working with children)
- Internally, through in-line education that regularly prompts users to check their settings or highlights reporting or blocking tools. Also internally by enforcing terms and conditions, age verifying users, and improving moderation and reporting functions on their sites/services.

6.3 Additional measures for the safety of all users:

Q125 we agree there should be minimum safety standards which digital products and platforms must meet. Such agreed standards can help drive universal take up of safety measures, and make an equal market place, and they can also help to raise and help communicate to users what their expectations should be in relation to particular services. Consistency would be helpful here as well as clear labelling, and Childnet are active in working to raise awareness about available tools to users.

There are additional measures that we agree with the highlighted need for, **Q127**, including the improvement of app rating in the App store, outlined in 6.4 and 6.5. Childnet support the visual descriptions added to Pegi ratings, though would like to see the reintroduction on the Contact with other users symbol, as we see that although most games provide some element of interaction with other users, not all parents are aware of this.

6.4 The role that applications and app stores play and 6.5 Safety values:

We support making **clear age requirements of apps** to users. There is a clear need for a clear system of age rating that users can trust. We have also raised this in the Technology Working group, highlighting how app ratings, which are applied by the developers answering questions, can often be very misleading, and signal a breach in the T&Cs of particular services. Like for eg, Facebook being rated 4+ in the Appstore. The potential contact risks, for example, have clearly not been taken into account, but also neither has the minimum age requirement of the app, and this is unacceptable.

6.6 Connected Toys

We welcome the review by the DCMS, and would raise the need for an education/awareness programme to support the potential purchasers of these toys.

Childnet response to **Chapter 7** 'Supporting children, parents and carers'

Background

Childnet agree that we need to start building digital literacy skills from a young age, and we have pioneered working to support young users, including Early Years, through the education system and through parents and carers. Resources like Digiduck's Big Decision, which has been translated and is used around the world, and Smartie the Penguin, have proved very popular, as well as the short guide for parents of 0-5s.

Schools are a key part of supporting children, and we have worked to support schools through, with support from the Government and the EU, providing guidance on preventing and responding to cyberbullying, and developing a toolkit for PSHE teaching on sexting, homophobic cyberbullying, peer pressure and self-esteem. As well as working directly with our target audiences in schools across the country, Childnet have developed a range of resources and programmes to support school communities; these target all age groups, including children with Special Educational Needs, as well as supporting teachers, parents, covering the range of issues young people face at different ages, discussing important issues around gender and peer pressure for example, and aimed at developing children's knowledge and skills so they can be empowered to use new technologies safely and responsibly.

With our UKSIC partners the SWGfL we have fed into and supported the inclusion of online safety in the Computing Curriculum, the duty to teach online safeguarding (in Keeping Children Safe in Education), and the SWGfL have supported Ofsted and the inspectorates of the devolved nations. As part of the UKSIC, the SWGfL host regular calls between the child protection teams of the four nations of the UK to discuss online safeguarding issues and initiatives. Schools are also very active supporting Safer Internet Day, and schools reported the benefits of doing so, with 48% saying that supporting the Day in school led to disclosures of potential online safeguarding issues.

We also support work outside of schools, developing key partnerships and engaging more actors into the work of empowering children online. Safer Internet Day was supported by over 1600 organisations from all sectors from right across the UK. Engaging with and helping to mobilise other voices that children listen to, for example, is a powerful way to reinforce learning. Training for social workers has been carried out as part of UKSIC, and more needs to done to reach other public sectors areas.

We also work supporting parents and carers, as well as foster carers and adoptive parents. Parents and carers have the key role to play, and we support them in our outreach programme, as well as the provision of key online information, and we reached 23% of parents with the Safer Internet Day campaign in 2017.

Childnet response to Chapter 7 Part 1 'Supporting children'

7.1.1 RSE and PSHE Education:
Childnet support the Government's policy here, as well as the move to make PSHE a statutory subject. We have been working in the area of Relationships and Sex education, and are currently developing a range of resources to assist the teaching around online pornography, body image and healthy relationships. We have been conducting focus groups with children and young people across the country, and have issued a survey of teachers/schools to find out more about what is currently good practice, what good examples they can share, and what they need to support them to teach in this area. We are also commissioning a survey of children around healthy relationships, which we will publish on Safer Internet Day 2018.

7.1.2 Digital literacy:
Childnet support the development of children's digital literacy, including critical thinking skills. Childnet launched the Trust Me resource, a free resource for primary and secondary, to help develop these skills, covering a wide range of issues, including content, such as advertising, and contact, including grooming and radicalisation.

Childnet also work to develop digital citizenship, through its wide range of programmes and resources.

Childnet's education work has been supported in a range of ways, with funding from Government, form the EU, from industry, and charitable trusts. All of these have a role to play in supporting these initiatives.

7.1.3 The wider role of the education system
The UK Safer Internet Centre plays an important role, and this is recognised in the Internet Safety Strategy, referring to the training, awareness, tools, policy support, and specifically 360 Degree Safe (used by over 12,000 schools in the UK), Safer Internet Day, and the more recent development of a competency framework, the summary as part of work for the UKCCIS Education working group.

The work covers all ages of children and young people, supporting staff, children and parents and carers, as well as supporting the inspectorates.

7.1.4 Other ways to support children:
The BBC are highlighted in the Strategy, and they have played a vital role in public awareness, particularly on Safer Internet Day, where their activity has provided oxygen to the efforts of others across the country, helping to reinforce other activities taking place in school and elsewhere.

Childnet welcome the particular mention of peer education, and the Childnet Film Competition and the Childnet Digital Leaders Programme. The Childnet Digital Leaders Programme has been enthusiastically taken up by both primary and secondary schools, and we currently have in excess of 4,000 digital leaders right across the UK, and plan to significantly grow this number. We agree that "there will be significant value in DCMS encouraging and supporting peer to peer support programmes like these that are specifically focussed on online safety"(p31). We see that an 'online safety peer to peer development scheme' (Q135) is an effective way of helping children stay safe online. But it also offers much more than this.

The types of children that can benefit from such a programme is broad (Q136), from primary school, right through secondary school, boys and girls. We also have some Special Educational Needs schools who have joined the programme, as the programme can go at the pupils' pace, and we are keen to explore how we can make amends to the programme to provide something specific to this audience. The nature of this approach can mean that peer education can work across a wide variety of child groups.

Technology has a role to play in supporting children develop their digital literacy skills (Q137 do you agree). We know, and research supports this, that children are generally very positive about their online experiences, and relish the chance to be constructive digital citizens (for eg, in the literature review by the UKCCIS Evidence Group, 'Children's online activities, risks and safety', p18). In March of this year, we were able to share the Government's Internet Safety consultation with the Digital Leaders, and share their collated responses back to the DCMS. We were also able to ask them questions to dig deeper into the issue of Livestreaming, and the programme can also provide in this way a meaningful youth participation, where young people can express themselves in the public domain.

We support the amplification of existing initiatives that make children and young people agents in this area. We need to provide positive opportunities for young people to participate in order to help them put their online learning into practice. They need opportunities to have their say and play their part in creating a better internet. We know that the most effective way of educating young people to be safe and responsible internet users is to empower them with positive messages that model good behaviours and promote a kind and supportive ethos online, giving young people responsibility for creating a more positive digital culture.

Childnet support the other areas discussed in the Strategy, including libraries, sports clubs and civil society (eg the Scout Association, Girl Guiding UK). For Safer Internet Day, all these stakeholders have been key participants and supporters, and the reach and impact of the Day is as a direct result of all these key stakeholders getting on board and effectively collaborating for this common cause.

Childnet response to Chapter 7 Part 2: 'empowering parents and carers to help children'

Childnet support the Strategy's concern with how parents, carers and teachers can be empowered to talk to and with children about internet safety. We also see that a role here can be played by children, and the Digital Leaders do run sessions for these audiences. A range of methods are necessary to reach what is a diverse audience.

A range of support is available for parents in the form of information and advice. And schools play a crucial role in sharing information with this audience, and is seen by parents as their preferred route to find out about this issue. There are still gaps in provision. We look forward to participating in the UKCCIS review of online safety materials and the identification of any gaps in resources, as well as continuing our work on ensuring parents and carers know what is available and being able to access the support they need.

7.2.1 Support for parents

In our response to the consultation in March, we explained the benefits in reaching out to new parents, and we are delighted to see this highlighted in the Strategy. Evidence points to the need to make this intervention.

We have always looked to reach children early, when their relationship with technology is in formation to help establish positive behaviour, and the same can be applied to new parents, as they are receptive to information and their parenting approach is in formation.

Health and early years provide new routes to reach these parents that are not currently being capitalised on. For example, key health professionals (health visitors, GPs) and early years professionals (children's centres, nurseries, baby and toddler groups, playgroups). The ideas outlined in the Strategy, such as NCT, Sure Start Centres are welcome.

7.2.2 Technology solutions for parents

Childnet agree with the approach outlined, of working to raise the level of awareness about the products available, although this does not need to be exclusively for the most innovative, as the most effective/trusted tools are important too.

We support consideration of different age-groups across digital products and we continue to be active in raising awareness to parents and carers of existing tools available.

7.2.3 Digital skills

Childnet already work with industry and other organisations to push for safety messaging built into to online platforms, including being provided at timely moments, to assist parents and others to stay up to date and make good decisions.

7.2.4 Troubled families

Childnet and the UKSIC are ready to support the Government's Troubled Families scheme – the SWGfL have been running training for child welfare professionals across a wide range of areas, and are well-placed to support this work.

7.2.5 Looked after children, children in need and care leavers

Childnet have already produced guides for foster carers and adoptive parents, and working with adoption organisations, run training sessions for adopting parents. We recognise this is an important area to support.

Childnet response to **Chapter 8** 'Responding to online harms'

Childnet response to 8.3 'Police response to online hate crime'

"As part of this Strategy, the Home Office are creating a new national police online hate crime hub" (p37)

The new online hate crime hub will need enough support to ensure that this includes the experience of children and young people in its remit, and also includes an educational goal to raise awareness around the issue, the reporting hub and how it can help. Until now Childnet has been promoting TrueVision to users that want to report online hate to the police.

In February 2016, for Safer Internet Day, the UK Safer Internet published a report, Creating a better internet for all, which outlined young people's experiences of online empowerment and online hate. It found that 82% of young people (13-18) had seen online hate in the last year. Most young people ignore it when they see it (55%), but the need for education around this issue is clear, as most (58%) who had been exposed to online hate said they wouldn't know when something breaks the law, and over a third (36%) said they would like more information about what to do about online hate and 75% said that more needs to be done about it.

Online hate does concern and affect young people, and 35% worry about it, and 74% said it can make them be more careful about what they share online, thus impacting on their freedom of expression.

Childnet response to 8.3 'Online dating and networking sites'

"we will consider whether there is a role for companies to provide appropriate messaging, and to take a stronger line in terminating accounts belonging to young people" (p38)

In relation to online dating and networking services, we believe that there should be a minimum age rating (Q140) for social media and application services enabling contact between users on a sexual/romantic basis, and the age rating should be 18 and above (Q141).

We agree that Q143 'adult-oriented applications or services with terms and conditions applying to users over 18 should be subject to age-verification' and this is because we know that this is possible – we see this in online gambling, removing the content bar on mobiles, and we will see this in relation to age-verification required to access on pornography. We see, Q144, that companies have a responsibility to ensure young people don't use adult dating/contact between users on a sexual romantic basis. The steps companies can introduce are age verification, making it easy for users to report under age users, terminating the accounts of known under 18s, and we believe there is a clear incentive for the providers of these services to carry out these checks and have these procedures in place.

Aspects missing from the Internet Safety Strategy

The consultation misses a few key areas which would make a significant difference to making the UK the safest place in the world for children to go online.

These missing areas include:

- The Children's Workforce
- Reporting Helpline for harmful content
- Other areas not discussed:
    - mental health of young people, and we assume this is due to the forthcoming green paper on this issue. We would encourage the results of both consultations to inform each other.
    - Online child sexual abuse: this is referred to as a Home Office matter, but clearly is part of the discussions that falls under the remit of UKCCIS (reformed or not). Areas relating to radicalisation/violent online extremism are also relevant to UKCCIS too.

Children's workforce:

Another priority area, and one in which research is telling us that we need to have more focus on – the wider children's workforce. These are the people who are typically on the frontline of online safety, providing advice, guidance and support, and dealing with the fall out, often safeguarding issues, from the latest online services. These professionals need to have the necessary skills and support in order to recognise, respond and resolve online safety issues. Section 7 includes details and recommendations for those supporting children, specifically early years and schools in England, the UKSIC would like to see this extended to the entire children's workforce.

Evidence base:

- Ofsted concluded in 2010 in their landmark report 'the safe use of new technologies' that "The weakest aspect of provision in the schools visited was the extent and quality of training

provided for staff. It did not always involve all the staff and was not provided systematically".

- According to UK Schools Online Safety Policy and Practice Assessment 2016, an annual assessment authored by Plymouth University and published by SWGfL as part of the UK Safer Internet Centre, **staff training remains consistently a weak area** with "Almost 50% [of schools] have no staff training to date around online safety". The latest 2016 assessment is based on data from 10,500 schools.
- It is therefore surprising that the Internet Safety Strategy does not consider this an area for focus or improvement.
- Anecdotally, the UK Safer Internet Centre Helpline is facing rising calls from the entire children's workforce about online safety related issues.
- UK Safer Internet Centre recommends that this is an area of great concern and warrants inclusion in the Internet Safety Strategy.

Current provision:

- Staff training is consistently a weak area for schools.
- Other key sectors working with children are not consistently addressing these issues.
- The UK Safer Internet Centre offers:
    - Online Safety Live: free training events reaching over 10,000 children's workforce professionals since 2013 across the UK
    - Bespoke staff training in schools
    - Free teacher training resources and advice
    - Professionals Online Safety Helpline (the UK's only specialist online safety helpline)

Gaps/ Solutions:

- High quality training for all school staff is needed; there may be opportunities in initial teacher training and CPD.
- Training and support for the wider children's workforce, for example: health professionals (GPs, CAMHS, health visitors, school nurses, community nurses), social services (social workers, foster carers, family support workers, children's homes), early years professionals (children's centres, nurseries, childminders), youth workers, young offending teams.

Reporting helpline for harmful content:

The public can report illegal content to the IWF, and professionals working with children can report to POSH, but for children and parents and carers, there is currently nowhere they can report to if they are unhappy with the response they have had from the social media provider. We propose the extension of POSH's remit to cater for children (or at least acting as a referral/support for existing child helplines) and parents and carers (again, potentially acting as a back-end for other parental helpline services). This would need to be properly resourced. POSH is a well-respected helpline in the eyes of industry and the audience they serve. They are also highly respected internationally, and have worked with NetSafe in NZ, the Office of the eSafety Commissioner (Australia) and

iCanHelpLine in the US. They also operate the separate Revenge Pornography Helpline, and again have supported international efforts in this area.