children's charities' coalition on internet safety
10, Great Queen Street, London WC2B 5DG

Submission to DCMS concerning the Internet Safety Strategy Green Paper

A crisis of confidence in self-regulation

1. Self-regulation and voluntarism have been the basis of successive governments' policy towards the internet for over twenty years. This is the case both generally but also specifically in relation to the safety and well-being of children as internet users[1].

2. The result has been a succession of government sponsored codes of practice and initiatives, none of which have had any binding force[2].

3. In relation to these codes and initiatives no reliable way was established to enable UKCCIS or anyone else to determine whether or not *any* online business *ever* followed or acted upon *any* of the suggestions that were made in them. Much less was anything ever put in place to try to assess the impact of the efforts being made.

4. We have been able, on an ad hoc or intermittent basis, to see what a small number of individual companies have done and in certain cases, for example with the mobile phone network operators, it has even been possible to test some of their specific claims, but that's as far as it has ever gone, and it is a long way short of what is needed.

5. What can be said with certainty, however, is that the codes and initiatives promulgated hitherto have plainly failed to convince the public, parents or young people themselves that everything that could be done to keep children safe when they go online is in fact being done. Parents are now more worried about harms that might befall their children on the internet than they are about them engaging prematurely with alcohol or tobacco[3]. As the survey published by DEMOS on 30th November 2017 also illustrated, across a broad range of issues there is a high level of anxiety among the public about a number of online challenges[4].

6. Add all this up and there is plainly a crisis of confidence in self-regulation.

---

[1] Around 1 in 3 of all internet users in the world are children. This rises to nearly 1 in 2 in parts of the developing world. In the richer OECD Member States the numbers hover around 1 in 5. Thus, whatever else one might believe, want or imagine the internet to be it is unquestionably a medium for children and families as much as it might also be many other things.

[2] See list in Appendix 1

[3] http://www.telegraph.co.uk/news/2017/02/27/parents-must-prepare-have-uncomfortable-conversations-sexting/

[4] https://www.demos.co.uk/project/public-views-on-technology-futures/

A near total lack of transparency

7. At least part of the crisis can be attributed to the fact that no other industry of comparable size or importance operates with such a near total lack of transparency or accountability.

Facebook refuses to co-operate

8. In 2013 the Government, via the Evidence Group of the UK Council for Child Internet Safety, asked Facebook to provide data on the volume and nature of problems being reported by children and on how long it was taking the company to address them. A senior Facebook Executive eventually responded by saying they would not provide any information they were not *legally obliged* to publish, and they gave the following reasons:

    a. If they did it for the UK they would have to do it for every country in the world.
    b. These matters are commercially sensitive and because of this they are constrained by the rules of the New York Stock Exchange.
    c. There is a super abundance of data and sifting through it could be like looking for a needle in a gigantic haystack.

9. When faced with similar requests or enquiries other online businesses have said things like *"we are a global company, we don't collect the information in a way that would allow us to identify how many children in the UK are raising particular issues", "it is often hard to classify complaints under particular headings in any way that would be meaningful because a single complaint can cross several different categories" or "timescales can be very hard to judge".*

10. These explanations are unconvincing. Online businesses and businesses of every sort have been able to devise highly sophisticated customer relations management systems which can yield a rich and detailed picture of what is happening with and to their users.

11. Parents, children and policy makers are entitled to know how different companies are responding to UK children's concerns and if existing systems cannot collect and provide data that would enable them to make such an assessment the systems should be changed.

12. Given the power of the "network effect" it is not acceptable for businesses to say that if their customers are not satisfied with the service they are receiving they can always go elsewhere.

Dense opacity

13. Thus, against a background of such dense opacity, it is extremely hard to speak with confidence about which or what kind of online safety or child welfare policies are most likely to succeed or to say how we will know whether or not different policies are in fact succeeding to the fullest extent possible or at any rate to an acceptable extent.

14. For example, while companies may speak about increasing the number of staff deployed on moderating user generated content this is meaningless without knowing anything about the volumes staff are supposed to be addressing, what guidelines and policies they are meant to

follow, or how they are trained and supervised. Information without context can be close to valueless and may mislead.

15. With the increasing use of Artificial Intelligence to identify potentially problematic content or behaviour a metric which can assess its efficiency might be every bit as important as knowing how many human moderators can be brought to bear.

16. The Green Paper speaks about working with industry to produce an annual transparency report but, while welcoming the idea, it will be important to know how the yardsticks will be established. It should not be by the industry marking their own homework again.

17. While the proposal to introduce a duty or expectation to "comply or explain" in respect of complaints or requests received sounds interesting, without knowing more about the institutional, legal or empirical framework within which it will operate it is hard to say how valuable an innovation it might be.

The social media code of practice must have a strong enforcement mechanism

18. For this reason, and notwithstanding the wider point made below at para 53 we very strongly believe that the code of practice on social media which is to be issued under the Digital Economy Act, 2017, must be linked to a Regulator with clearly defined legal powers to describe minimum standards and enforce those standards using a range of tools including, for example, an ability to levy substantial fines. Perhaps the Children's Digital Champion recommended in the Report of the House of Lords Sub-Committee on Communications [5] could fulfil such a role.

There is more to internet safety than social media

19. The focus on social media in the Green Paper is understandable, and while many other issues are referenced in the Green Paper, if only briefly, none receive a similar amount of attention even though some are of the highest importance in the context of children's safety.

20. The lack of security standards for internet connectable toys is perhaps the starkest example. The "Appification" of the internet also has profound implications for children particularly in respect of the App Stores' responsibilities to ensure adequate security is built in to every App they promote or allow to be sold, that the product descriptors and how in-App purchases may be made are easily intelligible to children and parents and are *consistent* across the different Apps platforms. The spread of a variety of different types of gaming also needs closer scrutiny as does the way in which certain games appear to be socializing the idea of gambling among under 18s.

Anonymity, as such, is not the issue – it's traceability

21. The abuse of anonymity is not the prime concern in the context of many problems facing the internet today, in the sense that how a person presents or names themselves to the online world can be of secondary importance, particularly if there is no reliable way of authenticating or verifying the names being used.

---

[5] "Growing up with the internet"

22. Indeed, from a child protection perspective in some circumstances there is much to be said for children *not* giving out or publicising their real name.

23. As it is, at the moment, where prima facie evidence exists of a crime, regulatory infringement or other unlawful act, either in respect of a child but also in other types of cases, the cost, complexity and time taken to identify a suspect can be such that for many regulators, and particularly the police, only the most egregious incidents will be looked into or ones which have attracted the attention of the media. The rest will pile up in somebody's inbox.

24. Thus, what matters is that, if necessary, law enforcement or another regulatory body with a legitimate interest, can rapidly, inexpensively and reliably identify who the author of a particular act is if knowing that is required for the purposes of carrying out an investigation.

25. Alternatively, we will all have to learn to live with a constant buzz or background of illegality of varying degrees of seriousness as a permanent feature of online life. That would bring us to a sorry pass and we doubt the British public, Government or Parliament are ready to accept it.

26. Closer co-operation between online businesses and law enforcement, together with reforms of international processes may help but equally it needs to be recognized it is highly likely there are limits to what can be achieved in this way. Radical technical solutions need to be devised and deployed.

   A big levy or a small levy?

27. The Green Paper speaks about the possibility of there being an industry levy to finance a range of educational initiatives to improve young people's awareness of potential online harms and how to combat them, but goes on to say only that this "could in future be underpinned by legislation".

28. The fact that the online gambling industry has lived with an unrealised threat of a legally based levy in respect of its education and awareness activities is cited as a potential reason for not rushing to give an education and awareness levy any binding force. However, the gambling industry, and in particular its online wing, are well accustomed to working with regulators within tightly defined legal parameters. The opposite is true with online firms not involved with gambling, which is most of them.

29. Our view therefore is that if there is to be any kind of levy to fund education and awareness programmes, while it may be appropriate to exempt firms below a certain size, it should be established on a clear legal basis in order that the public, parents, children and the firms themselves should know precisely what is expected of whom.

30. The definition of who should pay the levy should also be broadly drawn and not be confined solely to social media. Any online business which acts in a way that attracts children to any of its sites or services should be expected to contribute something to the overall effort of keeping those same children safe on the wider internet.

31. The state has an obvious interest in and obligation to ensure every child in every school is provided with a proper grounding in media literacy and online safety. This will need to be

closely integrated into a number of modules within the PHSE and the sex education curricula as well as aspects of civics. We would therefore be concerned if there was a suggestion that activities of this sort were to become in any way dependent on the grace and favour of industry or any other non-sustainable or uncertain funding sources.

32. Linked to this obligation on the part of the state is a duty to ensure that school teachers and the wider children's workforce are properly trained, equipped and supported so they recognise the role the internet and its associated technologies play in children's lives and can provide an appropriate response as and when needed. Could the levy be used to develop professionally accredited programmes for these professions?

33. We therefore see the levy as primarily supplementing current existing public-facing education and awareness initiatives which would include both safety oriented messages as well as messaging around the benefits of the technology to children and how, for example, it can help them realise one or more of the rights they enjoy under the UN Convention on the Rights of the Child and other legal instruments.

34. It will be critically important for there to be thorough independent appraisals of all major education and awareness initiatives, whether funded via the levy or not. We need to know what works and what doesn't, and we need to know why.

35. Special consideration should be given to helping parents and carers appreciate how they, in turn, can best help their children stay safe when they go online and get the most out of what the internet has to offer.

36. Special consideration should also be given to groups identified as having a particular vulnerability in online environments.

37. However, the levy could also support the work of clinicians and professionally recognised organizations who can develop our understanding of and provide specialized or targeted services to children who may have been harmed by an online experience. This latter dimension is extremely important because there is still, as yet, not a great depth of knowledge about the nature of, and best forms of treatment for, some of the new forms of harm children are experiencing on the internet.

38. Organizations that can extend the range of services they are able to provide to potential child sex offenders ought also to be a potential beneficiary.

39. More generally, without knowing the potential scale of funding that might be generated by a levy it is difficult to answer many of the questions posed in the online questionnaire. At one level many of them sound marvellous and if there were unlimited amounts of cash we might suggest trying all or most of them but, absent that, the critical issue will be how different challenges are prioritised and *how* decisions are to be made concerning where the money goes. There are several different potential models and at this stage, again without knowing anything about the size of the fund, it is impossible to advance any firm conclusion.

A levy to fund independent research

40. Given the scarcity of funds elsewhere a separate levy should be established to create an independent fund to finance research into emerging technologies and trends, specifically with a view to monitoring how they impact on the safety and rights of children. Alternatively, such purposes should be included as a relevant category of the previously mentioned levy. Hardware manufacturers would be an obvious source of funding for some parts of the research agenda.

41. Such an initiative would also help avoid or reduce the Government's and public interest groups' over-reliance on information provided or published by businesses or industry trade bodies who are far from being disinterested actors.

42. If this is not otherwise required by the GDPR or the Data Protection Bill, 2017, currently before Parliament, or other laws or codes, all businesses in the internet value chain should be under an obligation to carry out child safety and child rights impact assessments in relation to their products and services. Part of the research that is carried out using funding from a levy could examine the quality of such assessments.

Have we got the right lead Department?

43. When one examines the activities of the Department that has lead responsibility for the internet and for UKCCIS, DCMS, measured by the numbers and activities of civil servants employed it is quite clear that the burden of the Department's work is about improving the UK's technological infrastructure and encouraging businesses to grow their use of cyberspace. These tasks do not always sit easily with a responsibility to urge businesses, simultaneously, to "divert" resources to regulatory or quasi regulatory or co-regulatory compliance activities.

44. The Green Paper itself reflects part of this tension when it reminds readers (p4) "The government's approach to the most serious online crimes relating to ….. child sexual exploitation will continue to be led by the Home Office. … appropriate links will be made where the (Green Paper) Strategy offers additional solutions to these problems, for example through online safety education." Yet the "appropriate links" seem few and far between. Different parts of the online child safety agenda are very tightly entangled. It is disappointing, for example, that illegal activity such as grooming has not been given greater prominence within the Green Paper. See also our more extensive comments on violence against women and girls at para 64 (below).

45. That UKCCIS has suffered from a chronic lack of resources more or less since its inception is self-evident.

46. A proposal to evaluate the efficacy of UKCCIS was mooted in 2015 but following a change in personnel it fizzled out and came to nothing. The importance of monitoring and measuring was heavily emphasised in the original Byron Review which led to the creation of UKCCIS. It was re-emphasised in the subsequent follow up report which was also conducted by Byron. Yet as Appendix 1 shows, monitoring and measuring have been almost entirely absent.

47. Moreover, typically UKCCIS Board Members only discover what the Government is planning to do in relation to online child protection at the same time as the general public i.e. when they see it or hear about it in the media.

48. In the Chancellor's Budget Speech on 22nd November 2017 a £500 million investment was announced to support "a range of initiatives from Artificial Intelligence, to 5G and full fibre broadband". We fully accept the importance of our economy keeping pace with technological developments and why it is necessary for public funds to be used in the way suggested by the Chancellor. But if you are sitting where we are £500 million is an eye-wateringly large amount of money when UKCCIS has been run on a shoe string and a lot of voluntary effort from Day 1.

49. Obviously, it is acknowledged that UKCCIS, as such, is, by a long way, not the only measure of the Government's commitment to online child safety. Through agencies such as CEOP and a variety of other mechanisms the aggregate amount is likely to be considerable.

50. However, aside from the budget announcement on 22nd November, only two days earlier the Prime Minister announced[6] a series of tech related initiatives, including one which will give "Tech City UK" £21 million to expand its UK network, and back in 2013 the then Prime Minister appeared able to find £50 million to get the global We Protect initiative off the ground. This does make one wonder what UKCCIS needs to do to attract a similar high level of attention, or else it raises the question of how much it is truly valued.

51. What the foregoing and many of the comments that follow illustrate is a much more fundamental problem about how the internet is managed in the UK.

52. The "dense opacity" surrounding major tech companies' operations has already been alluded to, however, as with the internet itself, the arrangements for supervising or intervening in relation to the management of the internet have grown up piecemeal, in an ad hoc fashion but against a prevailing, strong impulse of the Government not wishing to intervene. Thus, while elsewhere in the Green Paper there are references to a (non-statutory) Digital Charter and to what a Data Ethics Commission might achieve it is respectfully suggested that these may amount to no more than another set of expressions of hope as they cannot possibly be founded on any real knowledge of what goes on inside the businesses they seek to address.

We need a review of how we manage the internet in the UK

53. For this reason, CHIS is calling for the creation of an expert, broadly-based time-limited body with the necessary, personnel, resources and legal powers to require businesses operating online in the UK to answer a small number of questions[7].

---

[6] http://www.evoc.org.uk/noticeboard/notices/prime-minister-announces-new/

[7]
   a. What are the optimal conditions for managing the internet in Britain so as to ensure the internet is as safe as it can be for children?
   b. What information and what mechanisms are needed to reassure parents, children, the public and policy-makers that everything that can reasonably be done to keep the internet safe for children is in fact being done?

54. Based on their findings the expert body will make recommendations to Parliament on how we should approach internet governance in the future.

55. At the moment much policy seems to be driven by crises which, in turn, are fuelled by media headlines. We need to move away from that to evolve a trusted, respected and more stable mechanism which is very broadly supported by civil society, industry and public alike, and in particular by parents and children.

56. In the USA, in a briefing organized by the Congressional Internet Caucus on 8th September 2017, Professor Julie Cohen, Professor of Law & Technology, Georgetown University Law School, in a similar vein observed that the administrative arrangements which presently exist in America had not been "optimised for the information economy we are starting to have". Exactly the same can be said of the UK.

Restructuring UKCCIS

57. We are deeply concerned about the suggestion that "Children" may be dropped from the title of "UKCCIS" as UKCCIS adopts a wider brief. Despite the many shortcomings referred to above the simple step of removing children as a named, singular or particular area of concern, as suggested by the proposed removal, carries with it the risk that, without more, at home and abroad people will believe child safety has lost a degree of focus and priority. Notwithstanding our earlier comments about the weakness of UKCCIS, that would be an odd message to send out at this time. The answer is to strengthen the machinery not weaken it.

58. The legitimacy and importance of the other interests referred to in the Green Paper e.g. of older people, are not disputed but a way should be found to take them on board which does not at the same time suggest children are dropping down the ladder.

The international dimension

59. We appreciate that many challenges confronting society in relation to the internet will best be solved by co-ordinated, internationally agreed actions. However, that is not a reason for the UK not to explore and determine precisely what can be done within the limits of our own jurisdiction. Outside of the USA the UK is the largest and most valuable market for online sales and online advertising in the western world. This gives the UK considerable leverage. Moreover, paralysis within international institutions is often only resolved when an individual country develops, tests and promotes a well-thought out series of suggested solutions to pressing problems. As the We Protect initiative has shown, leadership from a single country can shape and drive global agendas.

Digital Economy Act 2017 and pornography

---

    c.   What minimum standards should be observed by different kinds of online businesses and how and by whom should they be overseen and enforced?

60. We were disappointed with the definition of "extreme pornography" which was adopted in the DEA 2017 and look forward to the review promised by Lord Ashton in his closing speech in the House of Lords. In addition, it is to be hoped that the Crown Prosecution Service will be able to revisit and update its guidelines for prosecuting obscenity cases.

61. We await the publication of the draft regulations that are to be issued under the Act and trust a way will be found to ensure that social media sites such as Twitter are required either to close down individual accounts or profiles that provide or promote pornographic or sexual services or ensure that such accounts are put behind an age gateway so that children will not ordinarily be able to access or view them. For the avoidance of any possible doubt: there is not now, nor has there ever been any suggestion that Twitter as a whole be restricted on account of the behaviour of individual miscreants.

62. That said, on a site or service that allows children as young as 13 to be members there can be no justification for allowing material only intended for over 18s to be accessible via a few desultory clicks of a mouse and ticking a box simply to declare you are over 18.

63. Indeed, under the new data privacy regime that will begin in May,2018, it appears it may be the case that *any* information society service which makes clear its content or service is expressly intended *only* for persons over 18, will be required to demonstrate that, being mindful of available technologies, they have taken all reasonable and proportionate steps to make certain their declared policy is being observed.

   Ending violence against women and girls

64. Whilst it is we recognised that children and young people can develop positive relationships online – the internet has also facilitated specific offending behaviour in the context of both intimate and non-intimate relationships. The online world allows perpetrators to act towards peers and partners in novel ways such as; humiliating them online, sharing false and offensive information and 'catfishing'.

65. Additionally, there are a range of online behaviours that enable better known forms of domestic abuse such as stalking and coercive and controlling behaviour. Perpetrators may monitor and/or restrict a young people's internet usage and monitor their whereabouts using GPS location trackers built into many mobile phones.

66. Whilst we support the commitment to apply legislation set out in the Violence Against Women and Girls (VAWG) strategy equally online as offline as well as the commitment to introducing new Stalking Protection Civil Orders, we question how this will be implemented and regulated in practice.

67. It is not enough to simply transfer current legislation online without a robust process to ensure that legislation set out in the VAWG strategy is being used effectively offline. We know that, despite the increased efforts across all agencies to tackle child sexual abuse and exploitation, the true scale of sexual offending against children and services they receive in response is still not fully known. Many victims of sexual offences do not report these crimes to the policei. Moreover, the data published does not always differentiate between the offences and outcomes as experienced by children and adults (ii).

68. We estimate that between 1 October 2015 to 31 September 2016 around 54,000 sexual offences against children under the age of 18 were recorded by 43 police forces in England and Wales. The offences include: child sexual exploitation, familial sexual abuse, sexual abuse by a person in a position of trust, grooming, rape, sexual activity, sexual assault, exposure and voyeurism, trafficking, and indecent photographs of children.

69. This number does not reflect the full number of sexual offences reported to the police as not all offences recorded include the age of the victim. It is vital that a process that captures all offences and appropriately safeguards children including 16 and 17 year olds, who we know frequently do not get the response that they need8, against this kind of harm is put in place before simply transferring the process online.

70. Furthermore, it is not clear who will be responsible for moderating, reporting, collecting evidence and referring harmful behaviour online. In the offline world, there will often be a known adult such as a parent, carer or teacher that a young person can report harmful sexual behaviour and instances of domestic abuse such as stalking and coercive and controlling behaviour too. Online, the methods of assessing and reporting these types of behaviours are not clear. Without the introduction of a streamlined reporting mechanism we are concerned that children and young people will not know where to report harmful behaviours and slip through the net.

---ooo---

1st December, 2017.

---

8 https://www.childrenssociety.org.uk/old-enough-to-know-better

[i] Disclosure or exposure? Why young people may not seek or want your help (at first), A Briefing for the Police March 2017 Dr. Sophie Hallett1 available from https://www.uobcsepolicinghub.org.uk/responding-to-cse/briefing-papers

[ii] MOJ report