Making IT
good for society

Response to Information Commissioners Office Call for evidence: Age Appropriate Design Code

BCS, The Chartered Institute for IT

September 2018

BCS, The Chartered Institute for IT
First Floor, Block D, North Star House, North Star Avenue, Swindon SN2 1FA

BCS, The Chartered Institute for IT

BCS is a charity with a Royal Charter. Its mission is to make IT good for society. It does this through leadership on societal and professional issues, working with communities and promoting excellence.

BCS brings together industry, academics, practitioners, educators and government to share knowledge, promote new thinking, educate, shape public policy and inform the public. This is achieved through and with a network of 75,000 members across the UK and internationally. BCS is funded through membership fees, through the delivery of a range of professional development tools for practitioners and employers, and as a leading IT qualification body, through a range of widely recognised professional and end-user qualifications.

www.bcs.org

Call for evidence: Age Appropriate Design Code
Section one: Your views and evidence
Development needs of children at different ages
The Act requires the Commissioner to take account of the development needs of children at different ages when drafting the Code.

The Commissioner proposes to use their age ranges set out in the report Digital Childhood – addressing childhood development milestones in the Digital Environment as a starting point in this respect. This report draws upon a number of sources including findings of the United Kingdom Council for Child Internet Safety (UKCCIS) Evidence Group in its literature review of Children's online activities risks and safety.

The proposed age ranges are 3-5, 6-9, 10-12, 13-15 and 16-17.
Q1 In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate you consider the above age brackets would be:
Not at all appropriate
Not really appropriate
Quite appropriate
Very appropriate

Q1A Please provide any views or evidence you have on how appropriate you consider the above age brackets would be of setting design standards for the processing of children's personal data by providers of ISS (online services).

The 5Rights digital childhood report comprehensively outlines of the requirements of each of these proposed age brackets. In addition, the Intelligent Risk Management Model from I-KiZ shows *"for younger groups technical tools are a key protective measure, as the children grow older their media literacy develops and their individual responsibility becomes more important. For adolescents their ability to manage risks on their own should be trained by media literacy education and should be supported by the design of the services themselves. The ability to make decisions on their own, and to weigh risks, develop individually and depend on personal maturity and conditions."*

It is appropriate that a new age bracket begins at 13 as GDPR has set this as the age of consent for data processing. However, for anyone over 13 it is important not just to guarantee data safety but to scaffold this transition and provide help when things go wrong.

Evidence from the Children's Commissioner shows young people are unprepared for a social media cliff edge as they start secondary school. This transition occurs between ages 11 and 12 which is within the proposed age bracket 10-12. While 8-10s use social media in a playful, creative way – often to play games – this changes significantly as children's social circles expand in Year 7. This is also a turning point as peers become more influential to a young person than ever before. Development needs do not necessarily always fall in line with age and will be also affected by other factors such as parental engagement and education, for example, although someone may be 16 years of age, developmentally they may be equal to that of a younger age.

Since education should play a key part in young people's awareness of the digital world, an alternative may be to look at splitting these groups according to key stages (early years, key stage 1, key stage 2, key stage 3, key stage 4 and key stage 5).

Q2 Please provide any views or evidence about children's development needs in an online context for each, or any of the above age brackets.

The aforementioned digital childhood report and Intelligent Risk Management Model both provide comprehensive evidence for this. It is important to note that the two youngest proposed age brackets will be much more dependent on parents/carers when navigating the digital world, as a result these services need to integrate their involvement although if this requires parent/guardian verification, the methods for implementing a robust system for this will be complex. Services such as Google Family Link have done well to incorporate parent/guardian involvement although it relies on the adult to have a relatively high level of digital skills themselves and since a lot of younger children will not yet have their own device, they may be using a device which belongs to an adult and therefore may not be set up for a child to use.

The Act requires the Commissioner to take into account the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code.

Q3 Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services).

BCS held a round table discussion which included discussion on this topic. It was suggested that the principles of the UNCRC provisionally stand the test of the digital age. Some of the language may need to be recast in the light of digital technologies – and in particular, with the longevity and persistence of digital content which is addressed within the 5Rights framework.
In summary, our discussion group noted that children do not see an online/offline world, only the world – and in that world, governments have an obligation to meet children's basic needs, and to help them reach their full potential. This means education and parental responsibility, but it also means providing help to children when they get into trouble.

Some elements of the UNCRC fit clearly within the realms of the online world, such as Article 16 – The Right to Privacy, and Article 8 – Protection and Preservation of Identity. Some specific issues, for example the right to remove, is not in the UNCRC (but is included in the 5Rights). Perhaps digital rights could become a subset of the main UNCRC — if this happens then it must be considered how they are implemented in the digital context and who is responsible for doing that.

We also need to be mindful that in assuring their privacy we aren't impacting on other rights such as:

Article 12 – Respect for the views of the child
Article 13 – Freedom of Expression
Article 15 – Freedom to Association
Article 17 – Access to Information from the Media

Ultimately, children must come before profit, young people need to understand that they own their own data and that they can withdraw their consent if they don't like what's being done with it, and children need to understand the issues raised when someone else has their data, and what it can be used for.

Previously the child was largely a passive recipient of rights, but in the digital world they need to take a more active role. And as children are full participants in the digital environment, the whole of society needs to be involved in their safe participation. Young people will not be able to take an active role in these matters if we do not enable them to understand the digital environment, for example, children need to understand what they are signing up for when they tick 'agree' to T's and C's. Child safe websites will need to look seriously and innovatively at how best they can communicate their T's and C's to children without expecting them to read and fully comprehend lengthy legal contracts.

Young people have a right to expression and also a right to relevant education to support them. If the code attempts to manage young people's data more efficiently then there needs to be a level of education provided because there is nothing in the curriculum which addresses this. Privacy policy should be understood, and education is key here. In the UNCRC both Article 28 (Right to Education) and Article 29 (Goals of Education) highlight the importance of this. More specifically: "It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and the environment." Article 42 acknowledges the Knowledge of Rights, if a child has no awareness of their rights in a connected world, they will simply accept whatever controls and prohibitions are placed upon them by both companies and government.

Q4 The Government has provided the Commissioner with a list of areas which it proposes she should take into account when drafting the Code. **Please provide any views or evidence you have on what you think the Information Commissioner should take into account when explaining the meaning and coverage of these terms in the Code?**

Default privacy settings; This should cover personal profile data, and platform interactions such as posts made and liked, and friends added.
The presentation and language of terms and conditions and privacy notices: This needs to be made accessible and understandable for all. There should be considerations of some uniformity of messaging across platforms to help young people familiarise themselves with this type of content.
Uses of geolocation technology This should include stating location of posts/messages, stating current location, or showing on a map.
Transparency of paid-for activity such as product placement and marketing This should include posts made not only by companies themselves but also individuals posts which are sponsored/advertising, accounts which are for marketing purposes, an explanation of how this system works.
The sharing and resale of data; Including who the data is shared with and sold to, and for what purposes.
The strategies used to encourage extended user engagement Variable rewards, notifications, auto play, infinite scroll.
User reporting and resolution processes and systems Reporting content vs reporting users and addressing the same people making different accounts to target certain individuals.

Q5A The opportunities and challenges you think might arise in setting design standards for the processing of children's personal data by providers of ISS (online services), in each or any of the above areas
Some platforms span a wider range of ages than the single age brackets outlined and so adhering to granular age brackets may be a challenge to implement, for example CBBC is designed for young people ages 6-12 – how can we ensure than young people navigate only the content which is designed for their age bracket? Research shows that the most popular platforms amongst children tend not to be services designed primarily for children.
Platforms in the past have used a get out clause in stating that their services are aimed at people over a certain age, and therefore they do not need to address issues arising from underage users. However, the reality is that young people *are* using the services, so what is required is either greater controls to stop children using them, or to have a content filter for them if they do.

BCS held a workshop in conjunction with the DCMS internet safety strategy team and it was discussed that the legal ramifications for breaking such a code of practice would need to be significantly increased to tackle the issues effectively, which will require statutory legislation. Service providers feel they are responsible to their clients and customers but are not then responsible for their actions afterwards. It was felt that there would be scepticism within technology circles to government guidance unless it was from something like GCHQ. SME's need to be considered with regards to how information is made available to them and it was agreed that gov.uk would be a good repository for guidelines.

As the online environment has matured and children have become increasingly prevalent users, services have often had to retrofit to create a suitable platform for young people, often in a manner which is against their commercial interest (and with no incentives to do so, or consequences if they do not). As many young people are using services which are not designed primarily for children, one of the challenges will be in ascertaining the age of the user in order to ensure they are getting an age appropriate service, for example, Facebook requires users to be above 13 but many users are under this age. The nuances of levels of privacy with the age brackets proposed will not be straightforward to implement.

However, the opportunities what would arise from these standards will mean that young people will be empowered on the internet, they will understand their rights and what to do if they are not being adhered to. They will be receiving an appropriate service which scaffolds them from childhood to adulthood and educates them on the risks whilst supporting them through challenges - the online environment will become a place that young people will be able to thrive more than ever before.

Q5B how the ICO, working with relevant stakeholders, might use the opportunities presented and positively address any challenges you have identified.

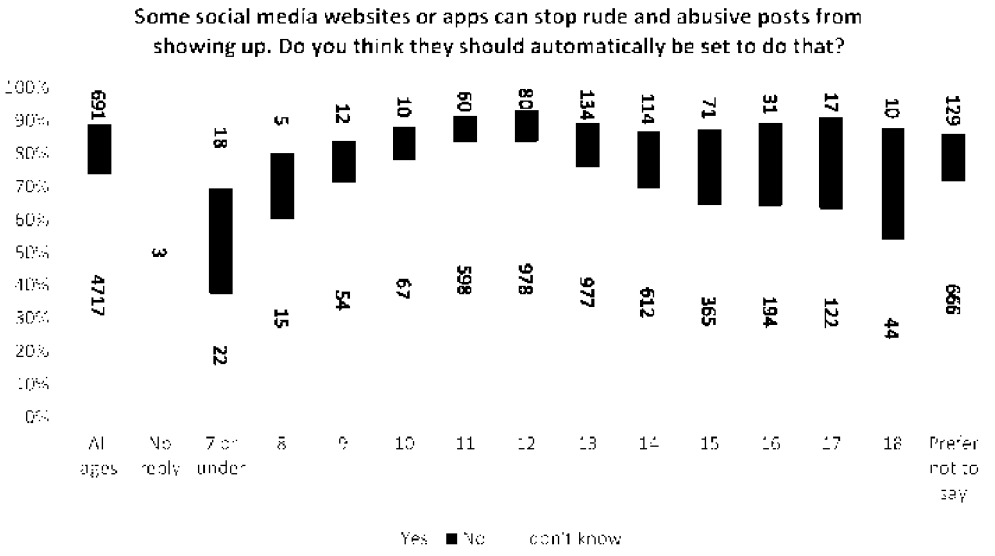
It will be necessary to frame any changes to the platforms as a way to enable young people and it is important to be realistic in how easy it will be to change things, as well as recognise the opportunity for legislation.

Q5C What design standards might be appropriate in each or any of the above areas and for each or any of the proposed age brackets

Default privacy settings For the youngest groups (under 13) profiles by default should set to private meaning all personal data is only visible to friends, this would also mean only being able to view messages from people whose friend requests have been accepted. As seen in the Facebook Kids service, an authentication process whereby a parent/carer must approve certain activity e.g. friend requests, posts etc. on their own device. Livestreams should also only be able to be seen by friends. Joint livestreaming is a bit more complex, especially if one person is younger than the other – in this instance it would be preferable to set defaults whereby the content is only able to be viewed by mutual friends or approved friends.

At the end of last year we conducted a survey to seek the views of school children on online safety, to coincide with the Government's consultation on its Internet Safety Strategy. The survey was sent to teachers in the Computing at Schools network, which includes those teaching at some 1,700+ primary and secondary schools in England, and asked them to get their school pupils to fill in the survey. The CAS network has been established for almost 10 years. It is a free to join, closed group, consisting mainly of primary and secondary state school teachers who teach computing, and who use the group for peer-to-peer advice, support and resources.
The survey was open from 27 November 2017 – 1 January 2018, and received 6,505 responses. The results show that young people would like a default setting whereby abusive posts are also automatically blocked from appearing.

QUESTION 4: Automated deletion of abusive/offensive posts



The presentation and language of terms and conditions and privacy notices This is related to the information provided in Q3, young people must be aware of their right and as a result must be able to understand the content presented in Terms and Conditions. This content needs to be communicated in simplified language (perhaps presented in video form and ensuring content is played from start to finish before accepting). Anything which is 'pre-selected' or has a default setting, should automatically be set to the most privacy friendly options. Schillings created simplified terms and conditions for a range of social media platforms which are much more accessible to young people. Community guidelines should also be simple to understand and have 'mandatory viewing' in the same way as terms and conditions, with clear examples of what would constitute a breach of community guidelines.

Uses of geolocation technology should not be offered as an option for youngest age groups, and default to off for older groups. If switched on, users should have the option to select which friends can view location and the locations should not be used for marketing purposes for those under 16 as evidenced in our YouGov omnibus poll of the UK public regarding the age of data consent which shows that the UK public believe this should not be happening until at least age 16. Privacy notices often use tactics to sway the user into choosing the most invasive options and making it more difficult to choose options which preserve privacy. The 'accept' buttons are often coloured and quick and easy to click on whilst the method to opt out requires numerous clicks into pages of settings to change defaults. This should be reversed so that the easiest options for young people are the options which preserve their privacy to the maximum.

Transparency of paid-for activity such as product placement and marketing The user should be made aware of what data is being collected from them and what it is being used for. Marketing services should be acting with transparency by explaining why a person is seeing the adverts which are presented to them, this will help educate them on what data is being collected about them and how it is being used. Platforms also need to clearly show which posts are sponsored/ads. The advertisements shown should be age appropriate, a number of gaming apps have been known to present young people with advertisements for sexualised games which is unsuitable. There should be a transition from no personalised marketing for the under 16 age groups and then services should let young people choose how their data is used to personalise advertising, this means prioritising privacy over profit.

During the GDPR update, Facebook's 'accept screen' had a default 'on' switch for advertisements based on data from third parties. It sold this concept by telling the user 'ads will be more relevant to you' and stated that if the user turned it off, the down side is they will see ads which are 'less relevant' but there was no explanation of any of the down sides to turning it on. This is not a transparent process and so for children within all the age brackets this should bet set to 'off' with a mandatory view video explaining the third-party involvement and what this really means for them. Instead of saying 'ads will be more relevant to you' which is leading the user to opt-

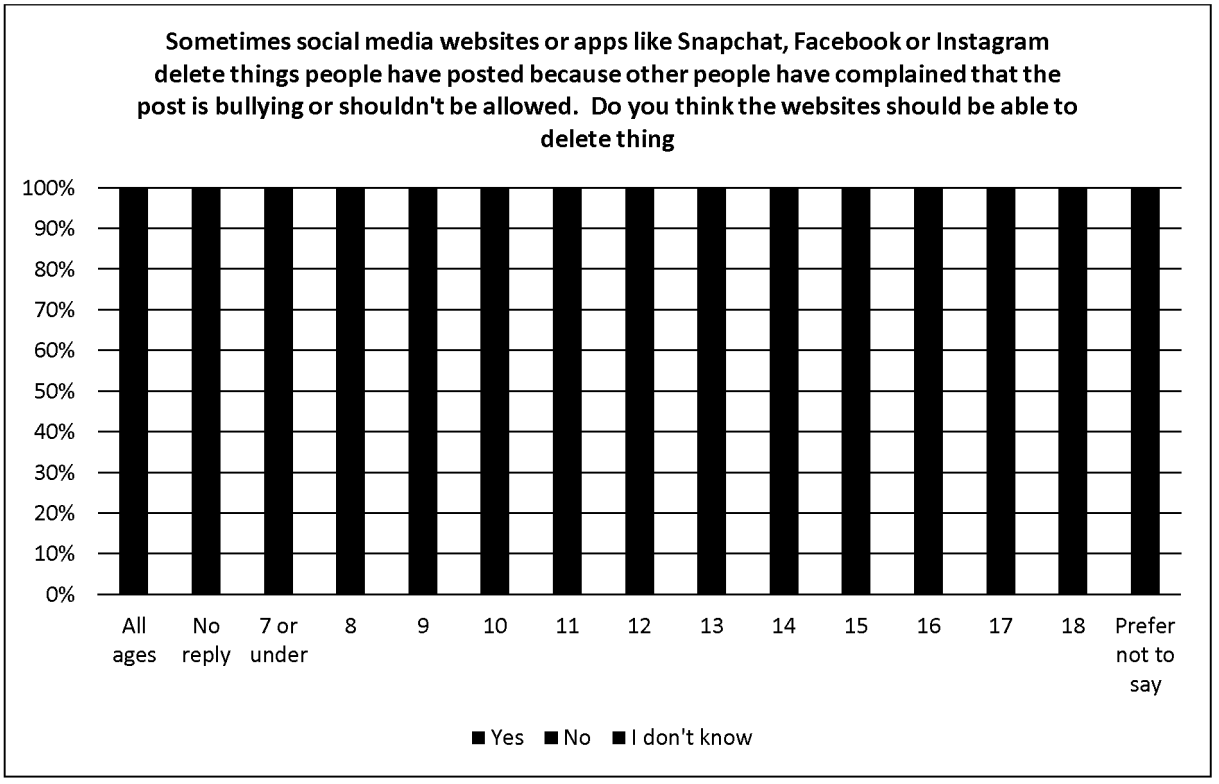
in, it should simply have factual statements such as 'ads will be based on data we have collected about you' or 'ads will not be based on your data'.

The sharing and resale of data; As stated above, we carried out a YouGov omnibus poll of the UK public regarding the age of data consent and our research shows that the UK public believe this should not be happening until at least age 16.

The strategies used to encourage extended user engagement such as streaks, are redefining the meaning of friendship and sacrificing privacy – young people are exchanging passwords so that a friend can keep up their streaks for example when they are on holiday. Functions such as autoplay and infinity scroll should also be set to off by default to help ensure time spent on platforms is intentional. The colour of notifications could be set to something other than red, and services could enable a function whereby users can enable notifications from certain people only, and/or at certain times only. Young people are particularly susceptible to these 'sticky' features and variable reward systems, services should relinquish the idea of the attention economy and focus on delivering a simple service which does not manipulate the user into spending more time, or giving more data to, the provider.

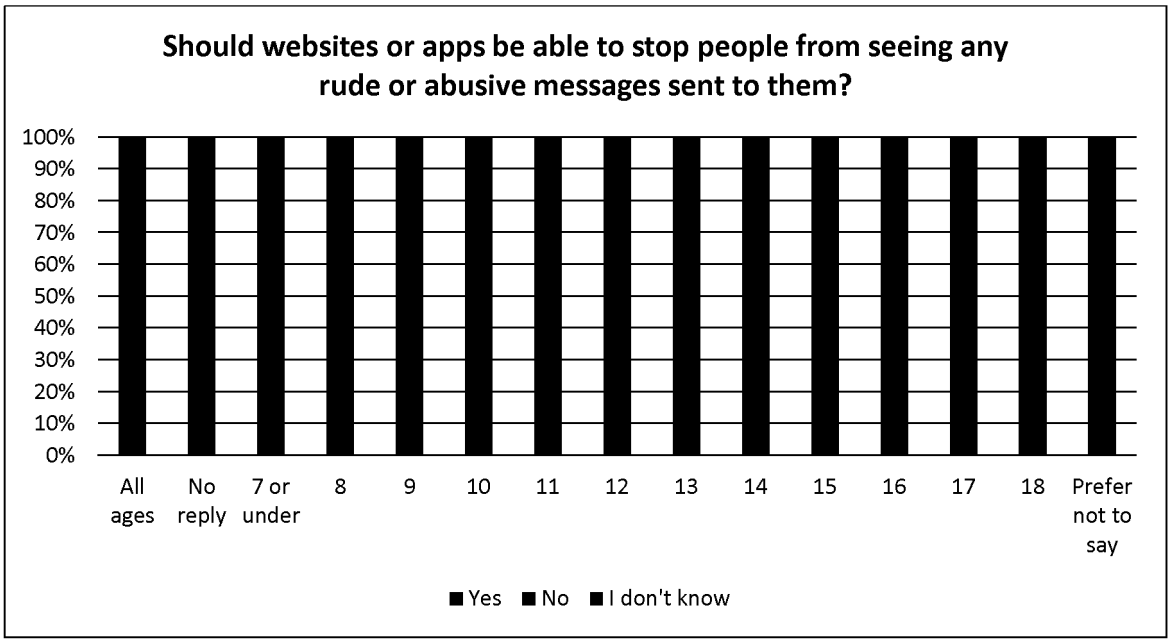
User reporting and resolution processes and systems Reporting and resolution requires transparency. The blocking of abusive messages will go some way to limiting the amount of reports which will be received by a service. Services should set standards to ensure resolution happens in a timely manner and to ensure that repeat offenders are sanctioned accordingly. Things which are inappropriate and reported by a user should be removed completely – not just removed from the view of the person who reported the content and real life case studies could be supplied for educational purposes. Livestreaming needs particular attention when it comes to moderation.

Our survey of 6, 505 young people and their views of online safety included two questions related specifically to reporting processes. Children, and younger children particularly, are in favour of social media platforms removing offensive or abusive content or direct messages automatically, without the need for a user complaint to be made first, and for this to be a default setting. As might be expected, the older the children become, the less sure they are that they want to be shielded from offensive or abusive content.



The issue of curation and censorship of online content is complex and evolving, but with regard to younger children lacks some of the dilemmas from the more general case, such as conflicts with free speech. It is an established principle that young children are shielded from inappropriate content. The principles set out in the United Nation's Convention on the Rights of the Child need to be interpreted into this context, which means a designed environment that is safe and appropriate, online or offline. This is a clearly-established set of principles, and the voice of children coming from these results reinforces those principles. Platforms need to be designed and operated to meet these needs.

In general, children are keen for offensive or abusive content to be removed by platforms without the need for a complaint to be made about them, though the strength of this opinion becomes progressively weaker as the children get older.



A clear majority of 8-13 year olds (72% on average) believe websites or platforms should be able to stop them from viewing abusive or offensive messages that are sent to them. This consensus decreases steadily as children get older, with 18 year olds being almost evenly split on the issue.

The ability to access advice from independent, specialist advocates on all data rights Who provides this service? How would a child know how to contact them? The sites themselves should signpost to this advice because first step to making this work is awareness raising, to help young people understand what their rights are online, so that they know what kinds of questions to ask and are able to recognise when their rights might be being breeched.

Q5D examples of ISS design you consider to be good practice.

SuperAwesome create 'kidtech' – services for young people (under 13) which are built specifically to ensure total digital privacy (COPPA/GDPR-K) for children and are a good example of services which carefully consider the experience for younger users.

Various other 'kids' platforms have emerged such as Facebook Kids (which requires a parent/guardian account for authentication and approval of interaction such as adding friends) and YouTube Kids – 'kids' versions of tools need increased integration with other products, for example, despite the fact a young person has a YouTube kids account, if they use a search engine to find video content then they could still get suggestions from the main YouTube service. If browsers aren't governed by legislation too, then results still may be inappropriate. GDPR ensures every single touch point can be controlled at the same time which means it will be an effective policy. Policy makers will have trouble making a difference unless something of that nature,

which encompasses all touchpoints, is implemented. It will be necessary to get consensus from device makers all the way through to content producers, and then support parents/guardians to implement it. You can put parental controls on via an internet service provider and this will filter content but if a young person downloads Instagram, for example, you can't control any content on that. GDPR is Europe-wide and therefore organisations could lose access to a big market if they are not compliant but with Brexit it will be hard to convince large platforms to make specific changes around just UK policy since they are so USA centric.

Good practice in smartphones could look something like a simplified OS which is put on the phone and allows you to slowly introduce certain apps and services, this is similar to the Google family link service, however but some the user implementation is complicated for parents to figure out, the service needs to be so simple for parents/guardians to control, almost to the extent where the adult enters the age of the young person and the providers sorts out the rest because fine-tuned controlling of each individual app/service separately is unrealistic. There is the potential for use of AI to govern access to all of these things at the same time – a system that learns how the touchpoints are being used and adapts accordingly.

Overall, this is an issue of continuing development rather than good practice. Any codes of conduct and policies implements need to be agile and flexible in light of new technologies and developments.

There needs to be better definitions of responsibility between platforms, users and developers, this isn't clear or consistent yet. There also needs to be agreement on definitions such as 'cyberbullying' and 'abusive content' as it isn't possible to uphold a code where there are varying definitions of terms such as these.

IT professionals need to see themselves as more than just 'tech people' – ethics and responsibility must be an integral part of these job roles now.

Q5E additional areas (not included in the list above) which you think should be the subject of a design standard.

In creating these design standards, the way these platforms interact with young people cannot be decided solely by policy makers and platform providers. These discussions must take on board the experiences of young people and a continuous dialogue with these groups is essential as technology changes so rapidly.

Q6b Brief summary of what you think you could offer

BCS is here to Make IT Good for Society. We promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

We have a membership base of 70,000; including experts within our Legal, Internet and ICT Ethics specialist member groups. We also have the Computing at School group which has 30516 members including numerous primary and secondary school teachers as well as 273 local hubs in which allow teachers and schools to network and share best practice.

Our policy team can run workshops and surveys with relevant stakeholders from these groups to provide evidence and insight.