Childnet International response to Consultation on Age Verification, Cross Media Rating and Classification and Online Social Networking

Childnet International

Childnet International is a registered charity, established in 1995, working with children, young people, teachers, parents and carers, industry, government and policy makers to help make the Internet a great and safe place for children, both in the UK and on a global level. For the past twelve years, Childnet has sought to promote the positive use of technology, by highlighting the creative and beneficial things that children are doing with new technology, as well as responding to the potential risks.

Childnet is pleased to respond to this consultation as set out below.

Cross media rating and classification:

1. Of which media rating systems are you aware in your country. Has there been an attempt to implement a cross-media rating system? If yes, what are the positive outcomes of it and its success factors? If no, what could be used as a starting point towards a cross media rating system?

- Internet Content Rating Association (ICRA)[1]
- British Board of Film Classification
- Pan European Game Information (PEGI)
- Rating of commercial content on mobile phones, using the IMCB[2] (UK's independent mobile classification body) as the classification board.
- In the US ratings are also provided by Commonsense media.

2. What are the main obstacles moving towards a pan-European cross media rating system?

There are two potential causes of confusion which could be obstacles in moving towards a pan-European cross media rating system, different cultural norms with regards to the suitability of content and the fact that there are some systems currently in use and a change to these could cause consumer confusion.

---

[1] ICRA (formerly the Internet Content Rating Association) is **part of the Family Online Safety Institute**, an international, non-profit organization of internet leaders working to develop a safer internet. The centrepiece of the organization is the descriptive vocabulary, often referred to as "the ICRA questionnaire". Most of the items in the questionnaire allow the content provider to declare simply that a particular type of content is present or absent. The subjective decision about whether to allow access to that content is then made by the parent

[2] The IMCB's main responsibility is to set a Classification Framework for commercial mobile picture-based content which is now available on many mobile devices. It is the responsibility of content providers to use this Classification Framework and self-classify their own content as 18 where appropriate. Where the content is classified as "18" under the Classification Framework its access will be restricted by the mobile operators until customers have verified their age as 18 or over with their operator.

3. What role should the different stakeholders play (industry, public bodies, etc.), towards implementing a pan-European cross media rating system?

Childnet believes that there is a need for the various different stakeholders operating in this area to promote what they are doing in this area. Ratings should be as transparent and easy to access and understand as possible, clearly marked on both offline and online products and content. Whatever system for rating and classification is used, there should be an emphasis on raising awareness about the ratings and how they work, and also on the need and importance of the ratings themselves to encourage consumers, including parents of users, not to ignore them.

Age verification:

1. Which age verification systems are you aware of? In which domains are they being used?

There are a range of methods for checking if someone is actually over 18, though it is more difficult to verify that someone is a child. Proving someone is an adult can be done through checking of a range of information databases, and there are systems that can do this, for example Experian. Many of the UK mobile operators use credit cards as the check to verify that someone is 18 years of age or older (as you need to be 18 to have a credit card in the UK), preventing access to 18-rated 'commercial' content to all users before this check has been successfully completed.

Examples of age verification of children include:

Offline verification by schools or parents, and one example of such a service is Superclubsplus (which came out of Gridclub). Here the children are authenticated by their school and teacher, and the application also needs the approval of the parent or carer. The advantage of these user verified environments for younger children are that it enables them to take their first steps in a more controlled and safer environment, enabling them to build competence and confidence with this type of interactive application. It is important to equip children so they are ready to leave such environments and enter less controlled environments.

There are some id cards that can be held by under 18s, such as citizen card, see http://www.citizencard.com/.

Childnet have met with one social network provider aiming at younger children who use biometric data once the identity and age of the user has been verified offline. Anne's diary, see http://www.annesdiary.com/, sends out a USB finger print reader to each user to ensure secure access. The logic here is that as most laptops and keyboards are beginning to provide finger print readers as standard, eventually they will they no longer need to send out these.

2. Do you think that these systems are efficient? If yes, please state why. If no, why do you think they are unsatisfactory?

These areas can provide safer environments and are normally targeted at younger users, ensuring their first steps online are in as safe an environment as possible. It can enable younger users to learn about interactive applications in a more controlled environment, building their confidence and competence in using these services safely and responsibly. However, it is important to assume that no age verification system can act as a substitute for other safety measures, tools and particularly advice to young users of their sites.

There are difficulties and an inevitable tension between the offline verification, and new technologies, mainly in the instantaneous nature of most online services, and the clearly slower process of managing effective offline verification by third party checking, although there are possibilities where services are accessed offline, for example at point of sale in a retail outlet.

Other potential obstacles include the scaleability of any offline checking system.

Online social networking:

1. What risks are minors most likely to encounter on SNSs? Are you aware of relevant research or statistics? If published online please provide us with the relevant URL.

Social networking sites, such as MySpace, Bebo and Facebook, are fantastically popular with children – even with children as young as 8&9 (despite the minimum age requirement of 13). These sites allow children to be incredibly creative online, keep in touch with their friends and express themselves using a whole range of different media and applications such as video, photos, music, message boards etc. However, it's important to recognize that while these are fun and offer great possibilities for children, there are potential risks including cyberbullying, contact by adults with a sexual interest in children and the misuse of personal information.

The risks facing children and young people using social networking services are outlined in the Home Office *Good practice guidance for the providers of social networking and other user interactive services 2008*[3].

Childnet were recently commissioned by Becta to produce the report *Young People and Social Networking Services*[4], which looked at the educational potential of social networking sites for education. The report also looked at the potential barriers to social networking sites use in education, and this included a look at the potential risks. The following text, explicitly addressing risk areas, is taken from the report.

It should be noted that this list of risks is not meant to be exhaustive and the risks of using social networking services very often overlap with issues that have been well addressed by existing e-safety advice and guidance, for example Childnet's award-winning Know IT All series of resources (http://www.childnet.com/kia/). This list looks at risks that are specific or pertinent to social networking services.

- **Misunderstanding the nature of the environment**

Within the report this refers to young people's knowledge of privacy and data management within services, and the impact this might have on both their personal safety and reputation. It also refers to how long public information can remain online, and highlights developing search technologies, such as sites specifically designed to search social networking content. The following information is provided to support young people to take control of their personal information and to better understand the online environments they frequent:

---

[3] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/social-networking-guidance pp16-20.

[4] http://www.digizen.org/socialnetworking/

““Site members need to be mindful of what they post, and how they behave publicly online. Anyone wanting to post pictures or video of friends should ask for their permission, and ensure they are not giving out inappropriate or personal information/content about themselves or about other people.

Service users should understand site permissions e.g. privacy settings and be able to use them effectively to regulate who gets access to information they post.

Basic permissions will be some variation on *private*, *friends*, and *public*. It is important to remember that 'private' information isn't necessarily private from the service provider, so information sent via instant messaging or social networking services' mail should be thought of in the same way as postcards are private. People who collect 'friends' or accept friendship from people they aren't really sure about may end up making personal information available to people and networks that they don't really know or trust. Members who don't really know and trust everyone on their 'friends list' need to treat any information made available to 'friends only' in the same way as they would treat public information.

Some sites have very complex permissions available to users. The *granularity* of site permissions, how simple or complex they are, varies from site to site. Permissions give members greater control over who can and can't see their information. Understanding how permissions work is important to all members - otherwise they may allow more people than they intend to see information, or be making information available to public search engines.

All internet users need to think about the information they post holistically. This means not just thinking about all the information they publish to one location or social networking services – but about all of the information collectively over all the sites that are used. Using search engines to search for themselves is an easy way of checking what information other people might find. Looking for specific information – such as home phone number, photographs, home address – can help users identify and take down inappropriate information – although making sure this kind of information is not posted in the first place is the most effective strategy. Many social networks will allow users to close accounts and permanently delete their information. It is important that users remember that publicly posted information may be accessible through Google cache records – which produce a copy of pages that have been searched - even after information has been taken down or deleted.

The law applies to social networking services as well as anywhere else, and certain content and behaviours are illegal. In addition services also have their own rules in their Terms and Conditions. It is important that users are aware that they can report to the service provider – it is good practice for service providers to have clear and accessible reporting functions available to their users – and also to the police. When reporting it will be useful to keep the evidence of what it is you want to report. For social network services keeping the url, or copying the relevant pages, or even printing the page to show someone can be useful ways of preserving this evidence".

Because user's privacy can depend on the robustness of the social networks privacy settings it is vital that these are secure. These tools are of fundamental importance to the safety and security of the services users and their confidence in the service, and

there have been reports of one or two incidences[5] where these systems have failed, and users' private information has been made publicly available.

- **Cyberbullying and anti-social behavior**

"Cyberbullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. Social Network sites can be abused in a number of ways. Most allow comments to be left (although these can often be restricted or require approval), and nasty comments might be left. People might use their own sites to spread rumours or make unpleasant comments about other people, or post humiliating images or video of them. Fake profiles can also be set up which might be used to pretend to be someone else in order to bully, harass or get them into trouble, or someone may find out or guess another users password and then go in and deface their profile or post inappropriate and upsetting content.

Video-hosting sites, such as YouTube, can be misused for cyberbullying, and pupils as well as staff have been victim to content posted up on such sites. Cyberbullying may take the form of video taken without the subject's knowledge, even from within class, that is then posted and shared, and/or acts of violence against people or property."

Further information and advice on cyberbullying can be found in the *Cyberbullying guidance* produced by Childnet International on behalf of the DCSF[6]:

- **Impersonation and identity theft:**

"Impersonation is when someone pretends to be someone that they are not online. They may pretend to be a real person, or they may invent a new identity. Fake profiles can be used to cyberbully, or be used by an adult to groom children (see below for 'grooming'). Everyone should understand that people online are not necessarily who they say they are. People might be dishonest about anything – where they live, what their name is, how old they are, what their gender is, their interests, and there is a broad range of reasons why they might be untruthful.

There are risks related to giving out too much personal information publicly on social network services. Identity theft can be one of the results of giving out too much personal information which is then used by others. There are also clear risks in giving out information which can enable others to contact and locate you offline."

- **Potentially illegal behaviour and illegal content:**

"Online grooming of a child is illegal in the UK. Online grooming refers to a number of techniques that are used to engage the interest and trust of a child or young person for the sexual gratification of an adult. 'Grooming' is a process of manipulation where an adult makes contact with a child in a online environment, then develops a relationship

---

[5] See http://www.brandrepublic.com/News/832186/Facebook-security-breach-reveals-users-private-data/, http://www.theregister.co.uk/2006/08/30/myspace_teen_data_hacked/ and http://www.crn.com/security/208402623 for some examples.

[6] See http://www.digizen.org/cyberbullying/fullguidance/

with this child, manipulating the child's emotions with the intention of arranging a meeting and sexually abusing the child. People who do this will often lie to gain trust, and may or may not pretend to be someone else. They may also try to use either threats or guilt to try and secure a meeting with the child or young person.

Illegal content in the UK includes indecent images of children, incitement to racial hatred, and criminally obscene content. Potentially illegal content can be reported to the UK's national hotline, the Internet Watch Foundation: see www.iwf.org.uk/. It is important that young people who are posting pictures of themselves or their friends online, think about the appropriateness of these images, and also be aware that indecent images of children (i.e. someone under 18) are illegal."

- **Sites or services spamming address book/contacts list**

"Users should be careful when they sign up to anything that involves giving access to an address book. Unscrupulous sites may spam contacts, for example inviting them to join services in order to boost their membership.

While it may be useful to search for those amongst your contacts/address book using the same service, it is important for users to be clear on what they are agreeing to allow the service to use that information for. "

- **Don't be bullied into being "friends" with someone**

"For social networking service users, deciding whether or not to accept a new "friend" can be a socially difficult decision. However, users should never feel bullied into accepting people. Accepting a "friend" and then later trying to delete that person from a "friends" list without anyone noticing is not a good strategy – although users should "unfriend" and block people when necessary, and report people who have broken the service's terms of use to the provider. Users should decide up front a clear framework for accepting "friends". This may vary from service to service - for example, users may decide to use a service account as a very public one and accept "friendship" from anyone who asks for it. Alternatively users might decide only to accept "friend" requests from people they know reasonably well, or from people they regard as close friends. When someone asks to be added to a user's "friends" list, they can stick to their rules for that service. Users should always ask people requesting friendship where they know each other from if they don't remember."

2. What controls, if any, should be available to parents over their children's SNS accounts? Should parents be allowed to cancel accounts or change profiles of their children?

There are undoubted advantages in offering choice to parents in terms of what controls they can have.

Research indicates that older children and teenagers use, and value, social networking services to experiment with their identity and develop independence and social skills, for example see: http://nms.sagepub.com/cgi/content/abstract/10/3/393

For younger children clearly, as in other areas of life, parents do exercise greater levels of control, and this is built in as part of the package for services offered to younger children, such as Club Penguin where pre-moderated services and template environments are used to restrict comments that can be made. This is an attractive option for those wishing their child to take steps in the area of social networking, but

who wish to ensure that at the early stages these steps are supervised to some degree. Superclubsplus's offline authentication and moderation is another such example.
In the cases of under age children using social networking sites, service providers already cancel the accounts of younger children who have misrepresented their ages in order to join services, once they are discovered.

Awareness and a greater understanding of the social network environments would be a key tool in assisting parents to support their child's experience on such sites. Parental involvement in the social network space can be a support for children, and at Childnet we do know of occasions where children have added their parents to their social network. Clearly it is vital to educate and empower young people so they are enabled to take responsibility for their own online activity as children develop their own networks. Parental empowerment is a key part of this discussion and Childnet has produced a key new resource to educate parents on young people and social networking, as it is important for parents to have an understanding of what such services are so they are able to discuss safe and responsible use for example, or be better able to support children if they get in into difficulties.

3. Which tools are the most appropriate to protect minors when using SNSs? What further steps should SNS providers take to reduce the risks to minors on their sites?

Site permissions and privacy tools and settings are critical to how children and young people manage their personal information on social networking sites. It is important that these settings are easy to use and understand. Permissions settings allow users to select levels of access to their content – for example, setting profile pages to private (only the owner) friends only (only consented and agreed contacts) or public (which may refer to all logged on service users or to internet users as a whole). Most services allow users to apply permissions to different elements of their content.

Childnet believe that all profiles should be private by default, to avoid the situation that we encounter in numerous schools that we visit, even primary schools, where children are unaware that the information they have put up on their profile is viewable to a wider audience than their school friends, ie the public. Making it private by default makes the sharing of you information a conscious decision, in other words an informed decision, as the user would need to choose this option. The Home Office Social networking guidance recommends that profiles are private by default for those users registering as under 18. Childnet believes that this is not enough, as without accurate or effective age-verification, and the protections thus relying on the self-declaration of age by the user, many children will register as over 18 and thus be denied the protections that are entitled to them. Some adults would also benefit by having to make a conscious decision about making their information public. In some research we carried out recently with the National Consumer Council, we heard from a young person on their view about age declaration for online services[7]:

'On all of my addresses I'm 20. Games, Bebo. If you want to go on a website, you lie about your age. They're not as safe for, like, six-year-olds'.
(Girls aged 11 to 12)

[7] See 'fair game?' Assessing commercial activity on children's favourite websites and online environments by Anna Fielder, Will Gardner, Agnes Nairn and Jillian Pitt, http://www.childnet.com/downloads/fair-game-final.pdf, p31

'If they give you extra for being 18 or over, then I put myself down as over 18'.
(Boys aged 14 to 15)

Education is also an important issue here, and it will have an impact. Nevertheless, if we wanted to be 100% certain that all children are aware of the status of their profile, and currently we find that many are not, then the default would need to be private for all users irrespective of their age but with still the choice to opt in to making your profile public.

Permissions vary across services, including what different groups (eg 'friends') are called. So it is extremely important that as well as a general knowledge of how permissions work that individual services provide clear information on their specific service.

Many social networking sites allow users to access or export information to third-party sites and services. If permissions and privacy vary from host services, users should be clearly alerted.

There are also tools to help users block contact from people who they decide that they don't want to hear from anymore, and also to allow the user to check or approve comments others are posting on their pages before they go up on the site.

Again, Childnet cannot stress enough the role of digital literacy information and education in safeguarding young people and supporting them to look after themselves and each other. An awareness of the safety tools available to them, is crucial, and advice about this should be clear, accessible and prominent on the service.

While clear onsite information is vital, ensuring that information is also 'timely' is extremely important. An example of a timely reminder could be information about safe posting of images at the point where the uploading is about to be done.

This information can be about how to keep safe while using the service, and it can be about the how to be responsible whilst using the service, and the terms and conditions or the rules of the club should be clearly explained to the users. This should not just be buried in the terms and conditions which the user needs to agree to in order to use the service, but it should be something that every user has to see and read.

There also needs to be information to users about the system of moderation on the service. If the service relies on user reports, then users need to know that they have this function, how to report and what content to report. If the service is pre-moderated, then it would be important for that to be well-communicated to the users and their parents.

The systems for reporting, the report abuse buttons are an important safety feature, whereby the user of the service can get help or report someone who is misusing the service. The reporting function and the language we use for it need to be as clear and easy to use as possible – this is even more important as children and young people are a very large percentage of the users of many of the services, and many parents who use this feature may not be familiar with these environments. Reporting is such an important function for child safety online, and it is vital that we encourage users to use it.

'Reporting abuse' is a broad term, and it has to meet the needs of the users, which necessarily covers a wide range of actions stretching from abuse of the service provider's Terms of Service, for example bad language or disrespectful behaviour, to

bullying and further into illegal activity such as unauthorised use of copyright material, grooming or posting images of child abuse images.

When the user feels that something is wrong, it is important that there is a clear, accessible and prominent place for the user to report to the service provider directly. As well as being used to report abuse, and this may cover a wide range of issues, both illegal and not, this reporting function will also be used by users who are not sure if something is abuse or not, and who are looking for confirmation that something is OK or not (and it may even be in relation to their own behaviour or posting).

The user will expect the service provider to have a lot of experience with reports such as theirs, and thus have the relevant advice or contacts to pass on, or be able to outline the best actions to take.

Thus, to reflect earlier Home Office good practice models, Childnet recommends that there is a clear, accessible and prominent system so that the user is able to contact the service provider easily from wherever they are within the service. It is also good practice, and this is reflected in earlier Home Office Good Practice documents, for the service provider to make information available and advise the user on how to report urgent and serious incidents, such as providing a child helpline number, and details of how to contact the police directly. We believe that this is crucial in making the whole report process effective and operators need to be as committed to providing this as providing a simple Report Abuse link to the police.

4. What should Members States do in order to improve the safe use of SNSs by minors? (E.g. legislation, co-regulation, awareness activities, introduction of the subject into the educational curricula, etc).

SNSs are part of a range of different applications that children are using online. It is important to encourage SNS providers to take child protection into account in the creation and management of their environments. The UK Home Office good practice document is a good place to start here. However, it is only useful if it is put into practice, and communicated widely amongst social network provider, and also that this is communicated to children, young people and their parents and carers to inform their expectations of such services and make them aware of the tools and advice available to them.

It is important that there is confidence in these services, and thus there is a need to communicate what SNS providers are actually doing in relation to protecting their more vulnerable users. It is also important that SNS providers are responsive to the needs of their users and maintain their confidence, for example by responding in good time to the reports their users send in.

Education and awareness about new media is crucial. E-safety has its place on the curriculum, given the importance of technology to children's educational and social lives. Within this there will need to be attention given to the impact of web 2.0 and the ability for children to create and publish content in the context of wider e-safety issues and the positive opportunities that these services can offer. Childnet's research report, Young People and Social Networking Services[8], looks at the formal and informal learning opportunities that SNS can support.

[8] See www.digizen.org/socialnetworking

Contact:
Will Gardner, Deputy CEO, Childnet International.
will@childnet.com