Online Safety Guidance

Content

Effective Date: 2 April 2019
Approved: Safeguarding Governance Group
Amended: 26 January 2016

1. Introduction

The term 'online-safety' is defined as the process of limiting the risks to children and young people when using any digital technology. Types of digital technology most used by young people include a wide range of social media platforms, online games, and websites, accessed via tablets, smart phones or, less frequently, desktops. See http://www.net-aware.org.uk/

This guidance is aimed at enabling all staff and volunteers (including trustees and interns) with signposts and advice and good practice to enable them to recognise the risks and potential dangers that children and young people can encounter in the online world. It will also help them monitor their own practices to minimise potential risks to children and families.

All staff and volunteers (including trustees and interns), secondees, agency staff, students, contractors and sole traders must read and understand the **Acceptable use of IT Policy**, which sets out guidance for the acceptable, safe and responsible use of online technologies. This is in place to help everyone understand all aspects of their duties when technology is involved. It should be read in conjunction with the NSPCC safeguarding and child protection policy and the what to do if you are concerned about a child procedure.

All staff and volunteers (including trustees and interns), secondees, agency staff, students, contractors and sole traders must understand that misuse of internet, digital and mobile technology may result either in disciplinary action being taken against them or with further services no longer being requested from the person in line with the **Code of conduct**. Those unsure of what constitutes acceptable usage of the internet should always check with their line manager or other responsible person.

3. Definition

The Byron Review (2008) identified that online risks can be classified in terms of content, contact with others and conduct of children in the digital world, illustrating that e-safety risks are posed more by behaviours and values online than by the technology itself. As such, the child could be a recipient, participant or actor in online activities posing risk.

The following are basic examples of the types of Online safety risk and issues that could fall under each category:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (Child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful Content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice

Contact (Child as participant)	Tracking Hacking Personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Terrorism Financial scams	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

DCSF, 2008 – Safer children in a digital world: The Report of the Byron Review

4. Prevalence and Legal context

For many young people, the online 'virtual' world is as real to them as the 'real' world, and digital technologies can offer children and young people opportunities to learn, communicate, be creative and be entertained. However, the digital world needs to be seen in the same context as the real world and we now have greater understanding on the extent of the risks posed to children and young people. Children and young people can be abused in their homes, community settings and educational settings through the use of digital technology by adults, other children or strangers [1].

- Children and young people are at risk of being sexually exploited online.
  This could involve a request that they commit a sexual act (s.10 Sexual Offences Act 2003), or by carrying out a sexual act believing that they can be seen by the child for example on a webcam (s.11) or making the child watch a sexual act (s.12). S.13 of that Act means that these offences can be committed by children and young persons themselves.
- Many children and young people have been 'groomed' online by adults often pretending to be other young people with the ultimate aim of exploiting them sexually. This can be via online chat rooms, social networking, email, mobile phones or stalking their online activities. S.14 and 15 of the same Act[2], facilitating a child sex offence or meeting following grooming can be committed even where the child does not actually meet up with the person.
- S.1 of the Protection of Children Act 1978 makes it an offence to take or possess an indecent image or pseudo image of a child or young person under the age of 18 years (s.45 of the SOA as inserted raising age from 16 to 18 years).[3] These offences can be committed by children and young people as well and even having an image on your phone without sending it anywhere would still be a criminal offence. In a ChildLine survey of
  13–18-year-olds, 60 per cent said that they had been asked for a sexual image or video of themselves and 40 per cent said that they had created an image or video of themselves (NSPCC, 2013). These all amount to criminal offences.

- Inappropriate (threatening, indecent or pornographic) images of children and young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites like YouTube which is again an offence under s.1 of the Protection of Children Act.[4] Some children and young people use the app "Snapchat" because they believe that their photos will disappear after 10 seconds however programmes exist which allow those images to be permanently saved.[5]
- Children and young people often use messaging apps such as Whatsapp but others such as KIK are often used by those looking to sexually exploit young people.
- Children and young people have been bullied by other young people via social networking sites, websites, instant messaging and text messages known as 'cyberbullying'.
- The dangers attached to gang culture can rapidly accelerate online as many gangs 'advertise' or promote themselves via websites or social networking sites, or if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites and images can be easily accessed online.

5. Personal: email account, social networking sites and devices – corporate communication

Corporate communications, such as emails or the transmission of documents, must not be sent over personal email accounts, or social networking accounts. Personal devices like laptops, mobile phones and other devices must not be used by staff for corporate business, including photographing children and young people for the promotion of the NSPCC unless used through an approved solution to isolate the device, such as Citrix. If you require a device for any activity within your role, you should request this through your line manager. Further information can be found in the **Acceptable use of IT Policy**.

6. Promoting the work of the NSPCC via personal social media accounts

As social media – websites and applications that enable users to create and share content or to participate in social networking – continues to grow, NSPCC employees are in a unique position to use these online networks to make a difference to the charity's work; by connecting with colleagues, reaching out to other professional networks, fundraising, or simply spreading positive messages about how we help children. It is important that NSPCC staff and volunteers are aware of safeguarding and reputational risks when using social networking sites or sharing content in a personal and professional capacity. All staff and volunteers should read and familiarise themselves with the **Social Media guidance for NSPCC staff and volunteers**.

7. Reporting online safety incidents

As employees of the NSPCC, we all have a responsibility to do everything possible to ensure children are kept safe from harm. If you come across anything online that could mean a child is at risk, you must report it as soon as possible. Remember that online safety incidents could involve a child, member of staff or other adult, refer to the table in section 3 for information on risks to children and young people and refer to the Acceptable Use of IT Policy for definition of appropriate use. Incidents may involve access to inappropriate or illegal material; inappropriate or illegal use of online technologies; deliberate misuse of the network; bullying or harassment using technologies or sexual exploitation using technologies. Please note that these examples are not exhaustive and if you are unsure what constitutes an online safety incident, please consult your line manager:

- Record this information using the **Safeguarding Incident Report Form**, making a note of the URL of the webpage or social media post that you are concerned about – it is very important that you **do not** take a screenshot.
- Send this information to the NSPCC helpline help@nspcc.org.uk
- The NSPCC helpline will take the information (known as a 'service request'), check if it is a known case to the NSPCC and will make a referral to children's social care (or equivalent in other nations) and/or the police. If the case is open to an NSPCC service, they will also inform that team.

The monitoring of online safety incidents is crucial for learning lessons and to inform future safeguarding actions. The NSPCC will review and monitor e-safety related safeguarding incidents and trends via the Safeguarding and Child Protection Leadership Group.

8. Good practice for those who work and volunteer with children and young people

The British Association of Social Workers' social media policy (2018) recognised the opportunities and challenges new technology brings to those working with young and vulnerable people. It highlighted the importance of professionals considering implications for their practice, their services and the interests of service users. They advocate applying the same principles, expectations and standards for interacting and communicating with people online as in other areas of practice; maintaining personal and professional boundaries in their relationships with service users and colleagues.

Professionals should review their personal content and ongoing usage of social networking sites as and when their professional responsibilities increase. Password and privacy settings should be applied (and regularly changed) in order for their profile and information to remain private. Friend requests from services users should be politely declined.

You should:

- Remember to appropriately set your privacy settings for personal and professional social networking sites.
- Ensure that your mobile phone or any equipment is password/PIN protected.
- Make sure that all publicly available information about you is accurate and appropriate.
- Remember that online conversations may be referred to as 'chat' but that they are written documents and should always be treated as such. Due regard should be given to anonymity.
- Make sure that you know the consequences of misuse of digital equipment.
- Be mindful that if you are unsure who can view online material, you should assume that it is publicly available. Remember that once information is online you have relinquished control of it.
- Make sure that when you receive any new equipment (personal or private), you know what features it has as standard and take appropriate action to disable/protect them.
- Make sure that if a service user requests you to add them as a friend on a social networking site, you should respond politely with the following wording:

"Thank you for your request on [insert as appropriate]. I won't be able to accept because this is my personal account. Please do though follow NSPCC and Childline on their social media sites so you can keep up to date with all the organisation's news".
If they are seeking support, you could also redirect them to Childline or the helpline.

You should **not**:

- Give your personal information to service users – children/young people/their parents/carers. This includes mobile phone numbers, social networking accounts, personal website/blog URLs, online image storage sites and passwords.
- Use your personal mobile phone to communicate with service users. This includes phone calls, texts, emails and social networking sites.
- Use the internet or web-based communication to send personal messages to children/young people unless this is part of official NSPCC business using professional accounts and devices.
- Share your personal details with service users on a personal social network site.
- Add/allow a service user to join your contacts/friends list on personal social networking profiles.
- Use your own digital camera/video for work – this includes integral cameras on mobile phones.
- Play online games with service users unless part of official NSPCC business using professional accounts and devices.

Good practice for fundraising volunteers

Fundraising volunteers will often have to use their own personal devices to undertake their activity on behalf of NSPCC. This may mean taking photographs at community fundraising events. Using images of children for publicity purposes will require the age-appropriate consent of the individual concerned and their legal guardians. Images should not be displayed on websites, in publications or in a public place without such consent.

Volunteers should always ensure that they:

- Obtain permission prior to using any media equipment or other device to take pictures while on external premises or facilities, checking out any external organisational policy in place.
- Seek permission in written form, given by an authorised and designated person who is aware of the reasons for the taking of the images and how they are to be used.
- Take images of crowds that show general images and do not focus in on any one person or child without permission.
- Try to keep children's faces obscure and away from direct identification where at all possible. (Even if permission is given by the premises/facility operator that the child or parent or guardian will be happy to consent for their child to be photographed.)
- Cross-reference the photographs with a code and not names and addresses, and never keep stored images with names and addresses attached or together.
- Make it clear to the parent or guardian who you are – show your identification, why you are taking the photos and their use, how they will be stored, making it clear that the photos will not be used for any business other than that of the promotion of the NSPCC.
- Delete images once used or emailed to an NSPCC staff email address.

Volunteers should also be familiar with good practice for privacy settings for mobile phone and social networking sites as outlined above. Communication with children and young people using personal mobile phones and email addresses for NSPCC activity should be directed through a parent or carer. For further advice/information, volunteers should contact their manager for support.

9. Children and young people – keeping them safe online

Children and young people go online to connect with friends, and make new ones, to browse the internet for information, chat with others and play games. They may:

- search for information or content on search engines like Google and Bing
- share images and watch videos through websites or mobile apps like Instagram, Pinterest, Vine and YouTube
- use social networking websites like Facebook and Twitter
- write or reply to messages on forums and message boards
- play games alone or with others through websites, apps or game consoles
- chat with other people through online games, games consoles, webcams, social networks and tools like WhatsApp

The Childline website contains helpful tips and advice for children and young people about how to stay safe online.

10. Parents/carers

Parents/carers or those with temporary guardianship for young people have responsibility for their children's access to personal and public computers, mobile phones and gaming platforms. This responsibility must allow for some degree of supervision and that both young people and their parents/carers are educated on the risks attached to the internet.

In particular, children and young people with additional vulnerabilities must be made fully aware of the dangers they face online and should have a greater degree of supervision to minimise risk to them.

These vulnerabilities may include:

- Special educational needs
- Physical/learning disabilities
- Not in mainstream education
- Are unable to fully understand the consequences of their actions
- Young offenders or affiliated with gangs
- Travellers with inconsistent access to education
- Have language barriers if English is a second language
- Are in short term accommodation or placements

The NSPCC has produced online safety advice to help them guide and support their child on online safety. These include advice on:

- Setting rules and agreeing boundaries
- Talking about online safety and getting involved
- Knowing who their child is talking to

- Checking content is age appropriate
- Parental and privacy controls

In addition, netaware offers advice for parents and carers on social networks and apps most used by children

11. Adults at risk

Some adults are more likely to experience abuse, harm, ill treatment or neglect than others, and are less able to protect themselves. This group of adults can also be vulnerable to online risks since they are more likely to experience abuse, and less likely to be able to take action to make it stop. Remember that this could be a member of the public, a service user, but could also be an NSPCC staff member, a volunteer or a fundraiser. For further information, please refer to the **Safeguarding adults at risk of abuse policy and procedure**.

12. Further information

Social media

For further information directly from social media providers you can visit:

- Facebook Safety Centre
- Twitter Safety Centre
- Pinterest
- Instagram Safety Tools and Privacy

Parents

Further sources of advice, information and support for parents:

- InternetMatters.org, which contains interactive information, advice and support for parents to help keep their children safe online.
- The Parents section of www.thinkyouknow.co.uk
- E-safety advice to parents/carers and foster carers produced by North Yorkshire LSCB.
- BBC Webwise – information on webcam and online safety
- Google offers a guide for parents on how to report abuse. They also provide information on how to report inappropriate content reporting abuse in their Safety Centre
- The Internet Watch Foundation (IWF) is the UK Hotline for reporting criminal online content, and works with the internet industry, police and international partners to get it removed. Reports to the IWF are confidential and can be submitted anonymously.
- Ofcom advice guides for parents
- O2 information – Keeping your family safe in the digital world

Children and young people

Further sources of advice, information and support for children and young people:

- Childline provide advice about a wide range of issues, and children and young people can talk to a counsellor online, send Childline an email or post on the message boards

- CEOP's Think U Know? website contains the latest information on the sites that children and young people like to visit, as well as guidance about mobile phones and new technology. The site is divided into age groups: 5–7; 8–10; 11–13; 14+. Most importantly, there is also a place that anyone can use to report if they feel uncomfortable or worried about someone they are chatting to online
- Childnet International is a non-profit organisation working with others to help make the internet a great and safe place for children.

13. References

British Association of Social Workers (2018) *BASW social media policy*. Birmingham: BASW

Byron, T. (2008) *Safer children in a digital world: the report of the Byron Review*. Nottingham: Department for Children, Schools and Families (DCSF)

NSPCC (2012) A qualitative study of children, young people and 'sexting'. London: NSPCC

[1] Reflected in the guidance are potential 'digital world' criminal offences as contained within the following:

Safeguarding Vulnerable Groups Northern Ireland Order 2007 Schedule 1;
Protection of Children and Vulnerable Adults Order (NI) 2003 Part IV Schedule 'offence against a child'; and
Serious Crime Act 2015, Part 5 Sections 66 – 69 'protection of children provisions'.

Bullying/Harassment

Protection from Harassment Order (NI) 1997 (bullying offences causing psychological harm ie cyberbullying); and Protection of Children (NI) Order 1978.

Emotional and Psychological Abuse

Offences Against the Person Act 1861, Section 120; and
Adoption and Children Act 2002

Snap Chat /Whats App

Malicious communications (NI) Order 1988 (text messages etc.);
Telecommunications Act 1984, Section 43 (sending offensive telephone messages); and
Communications Act 2013, Section 127 (sending offensive messages).

Grooming

Serious Crime Act 2015, Part 5, 66 – 69, Article 67 (sexual communication with a child); and
Sexual Offences (Scotland) Act 2009, Section 24 (child under 13) and Section 34 (for those above that age – communicating indecently).

Sexual Offences

Sexual Offences (NI) Order 2003;
Sexual Offences (Scotland) Act 2009, Section 21 (child under 13) and Section 31 (for those above that age – causing a child to engage in sexual activity); and
Sexual Offences (Scotland) Act 2009, Section 25 (child under 13) and Section 35 (for those above that age – exposure of genitals)
Sexual Offences (Scotland) Act 2009, Section 26 (child under 13) and Section 36 (for those above that age – voyeurism)

Photographs and Video

Protection of Children (NI) Order 1978, Article 3 (indecent photographs);
Sexual Offences (Scotland) Act 2009, Section 23 (child under 13) and Section 33 (for those above that age – causing a child to look at a sexual image (whether or not the image is moving)); and.
Serious Crime Act 2016, Sections 66 – 69.

[2] For Scotland refer to Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, Section 1

[3] For Scotland refer to Civic Government (Scotland) Act 1982, Section 52 & for children up to 18 - Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, Section 52

[4] For Scotland refer to Civic Government (Scotland) Act 1982, Section 52 & for children up to 18 - Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, Section 52

[5] For Scotland refer to Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, Section 1