

November 2011

# E Safety

Inter-agency Practice Guidance



Nottinghamshire  
**SAFEGUARDING**  
**CHILDREN** Board



NOTTINGHAM CITY  
**Safeguarding**  
**Children** BOARD

## Contents

	<b>Section</b>	<b>Page</b>
<b>1</b>	<b>Introduction</b>	<b>3</b>
	<ul style="list-style-type: none"><li>• Scope</li><li>• Background</li><li>• The Internet</li><li>• Acceptable Use Policies</li></ul>	
<b>2</b>	<b>Safeguarding Issues</b>	<b>7</b>
	<ul style="list-style-type: none"><li>• Exposure to Sexual Content</li><li>• On Line Grooming</li><li>• Contact between staff/volunteers and children/young people on Social Networking Sites</li></ul>	
<b>3</b>	<b>Indecent Images</b>	<b>9</b>
	<ul style="list-style-type: none"><li>• Child Abuse and the Adult</li><li>• Children and Young People who are the Subject of Abusive Images</li><li>• Guidance upon the Discovery of Indecent Images of Children</li><li>• Actions to be taken when an Employee has concerns about a Colleague</li><li>• Outcome of the Section 47 Enquiry.</li></ul>	
<b>4</b>	<b>Cyber bullying</b>	<b>12</b>
<b>5</b>	<b>Glossary of Current Legislation</b>	<b>13</b>

# 1. Introduction

1.1 The NCSCB and NSCB have agreed the following policy statement:

“Any person accessing / distributing / producing images of child abuse or grooming using information and communication technology (ICT) will be considered as a potential risk to children. This includes the use of computers, mobile phones, grooming through chat rooms and text messaging etc. A robust, coordinated multi agency response will always follow any such allegations coming to light”.

1.2 This practice guidance was developed by a cross-authority, multi-agency group. It provides guidance on effective approaches to e-safety for organisations in Nottingham City and Nottinghamshire.

It covers:

- awareness-raising for children and young people so that they are able to keep themselves as safe as possible when using the internet and other digital technologies
- policies and guidance to enable agencies to support the safety of children and young people in the digital environment
- the responses necessary when a risk to a child or a young person is discovered

1.3 E-safety is a safeguarding issue and all organisations need to ensure that existing policies can be applied to the digital environment. In order for this to happen, it is essential that these policies are regularly reviewed against this e-safety guidance and updated as necessary. This policy and guidance can therefore be used as a stand-alone document or it can be used to inform existing policies.

1.4 This policy and guidance should also be read in conjunction with the inter-agency NCSCB/ NSCB Safeguarding Children Procedures, which are available on the NCSCB web page and/or the NSCB web page.

## 1.5 Scope

- 1.6 The target audience for the practice guidance is staff and volunteers from all agencies and the voluntary sector working with children and young people who are resident in Nottinghamshire or Nottingham City. They apply to all children and young people up to the age of 18 years.

## Background

- 1.7 E-safety is defined as ensuring children and young people are safe whilst using all fixed and mobile technologies that children and young people may encounter, now and in the future, which allows them access to content and communications that could raise e-safety issues or pose risks to their well-being and safety (**British Educational Communications and Technology Agency - Becta**).
- 1.8 In addition, the UK Council for Child Internet Safety (UKCCIS) brings together over 170 organisations and individuals from government, industry, law enforcement, academia and charities, including parenting groups to work in partnership to keep children and young people safe online.
- 1.8 Safeguarding children and young people, including e-safety, is everyone's responsibility; e-safety is not a responsibility for just ICT staff. It needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of children and young people.
- 1.9 The Internet gives great benefits to everyone, most of all children. Yet with all of its advantages, it has disadvantages which can create dangers for children. It is critical that every parent, guardian and practitioner is well informed about the Internet and the possible hazards it creates for children. This practice guidance has been developed to raise awareness of the potential dangers and how to deal with them.
- 1.10 The Byron Review (March 2008)<sup>1</sup> concluded that there is a generational digital divide between parents/carers, children and young people and that many parents and carers are unsure about how to teach their children risk management skills when using the Internet. It is more than likely that such an observation will also be true for members of the children and young people's

---

<sup>1</sup> <https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00334-2008>

<sup>2</sup> <https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DCSF-00290-2010>

workforce. An additional follow up report asking “Do we have Safer Children in a Digital World?” (2) reviews progress since the Byron Review.

- 1.11 Children and young people generally have superior ICT skills to their parents/carers and to those adults that work regularly with them. However, children and young people do lack the ability to comprehend and assess risk, as well as clearly understand the implications of their behaviour.
- 1.12 The sense of uncertainty and anxiety that a parent/carer may feel is likely to be driven by a lack of knowledge and skills, and these feelings are heightened by media stories which link internet usage to abuse and anti-social behaviour. Overall, parents tend to equate their ability to protect their children when online with their relative skill levels, so children and young people of parents with few internet skills are potentially disadvantaged in terms of protection from the risks.
- 1.13 In terms of adults working with children and young people, it is likely that they may experience the same sense of anxiety, and on this basis it is essential that they receive appropriate information and training to raise awareness about e-safety.
- 1.14 Where possible work young people (and their families) should highlight the importance of E-safety and some of the basic measures that young people can take to promote this, e.g. how to set privacy settings and how to report concerns. Further information in this regard is available on the Child Exploitation and Online Protection Centre (CEOP)

<http://ceop.police.uk/>

## **The Internet**

- 1.14 As technology has developed, the Internet and its range of services can be accessed through various devices including mobile phones, text messaging and mobile camera phones as well as computers, notepads, notebooks, Kindles and game consoles. The range of devices that can be used to access the Internet is ever evolving. As a consequence it has become a significant tool in the distribution of inappropriate, abusive and indecent/pseudo photographs and video clips of children and young people.
- 1.15 The growth of Web 2.0 technology has led to the potential of what is called in the Byron Review ‘increased interactivity’. This means that children and young people will associate with each other and form friendships online in a way that is not replicated in age related off-line social friendship groups. This in itself poses new risks and challenges regarding the appropriateness of online contact.
- 1.15 Internet chat rooms, discussion forums, bulletin boards and social networking sites are used as a means of contacting children with a view to grooming

them for inappropriate or abusive relationships, which may include requests to make and transmit pornographic images of themselves or to perform sexual acts live in front of a web cam. Contacts made initially in a chat room or via a social networking site are likely to be carried on via email, instant messaging services, mobile phone and text messaging.

## Acceptable Use Policies

- 1.17 In general terms, an acceptable-use policy (AUP) is a document detailing the way in which ICT facilities may (and may not) be used by staff and service users, listing sanctions and procedures for misuse. An acceptable-use policy must be wide ranging. They are important as they set out the framework and principles which should support safe use of ICT.
- 1.18 An AUP must consider both fixed and mobile access to the internet, equipment provided by the service itself (such as PCs, laptops, webcams and digital video equipment) and equipment owned by service users and staff but brought onto the service premises (such as mobile phones, camera phones, personal digital assistants (PDAs), games consoles and portable media players). It should be flexible enough to deal with new and emerging technologies, such as Virtual Learning Environments (an interactive tool to support teaching and learning in an educational setting), but should also recognise the important educational and social benefits of such tools.
- 1.19 The NSCB and NCSCB strongly recommend that all partner agencies should develop an AUP tailored to individual users and/or stakeholder groups as appropriate. It is also recommended that agencies review how their network is monitored and use Internet monitoring tools that can block access to certain types of sites and audit internet history for specific periods of time and to identify an individual login.
- 1.20 All partner agencies of the Safeguarding Children Boards, should also have clear policies and procedures in place addressing the issue of employees accessing illegal indecent images of children. Managers should have a clear understanding of what procedure to follow should they be informed that one of their staff members is suspected of accessing such images either on a works or personal computer (see page 10).

## 2. Safeguarding Issues

### Exposure to Sexual Content

- 2.1 The risk to children and young people covers 3 basic scenarios where a young person is deliberately or unwittingly exposed to:
- adult content online
  - content depicting the sexual abuse of children
  - other sexually themed content that may cause harm to the child (e.g. sexualised pseudo-image of themselves).
- 2.2 Where there are concerns regarding online grooming and/or exposure to sexual contact, the NCSCB / NSCB Safeguarding Children Procedures should be followed. This may include a referral made to Children's Social Care where there is a risk of significant harm.

### On-Line Grooming

- 2.3 Online solicitation and 'grooming' are the most common forms of online child sexual abuse. Grooming refers to actions deliberately undertaken by an adult with a sexual interest in children, with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual abuse.
- 2.4 Online predators may follow a pathway from friend to bully in order to establish a degree of control over children. They will most often start out as 'friends' and then start to attempt to gain influence and control over the relationship.
- 2.5 Commonly online predators will follow a path of behaviour which will include:
- disguising or misrepresenting themselves as a child or using school or hobby sites to gather information about particular children, their locations or future events where the child may be present
  - suspicious online contact with a child, for example by asking a child sexual questions, to meet in person etc
  - causing a child to watch a sexual act, for example sending sexually themed adult content or images and videos featuring child sexual abuse to a young person
  - inciting a child to perform a sexual act, for example, by threatening to show sexual images of a child to their peers or parents.

## Contact between Staff / Volunteers and Children / Young People on Social Networking Sites.

- 2.6 Locally we have had a number of examples where contact between children and young people and staff/volunteers on social networking sites has created difficulty. Staff/volunteers should be cautious when using social networking sites outside of work and avoid publishing, or allowing to be published, any material that could damage their professional reputation and bring their organisation/agency into disrepute. As staff /volunteers may not be aware of how young people may be able to access their personal information, they are strongly advised to set their profile as 'private'. Staff/volunteers should not allow or seek access to profiles of children/young people that they work with, their families and or carers.
- 2.7 This would not preclude an organisation using social networking sites to undertake consultation or other forms of work with children/young people but such work should take place in clearly defined circumstances, endorsed by senior management within the agency and staff should not use their personal profile to undertake such work. The agency will need to ensure that issues in respect of professional boundaries and computer literacy of staff undertaking such work have been addressed.
- 2.8 Where there are concerns about the nature of contact between a member of staff/volunteer and a child or young person this should be discussed with the Local Authority Designated Officer (LADO). The contact details for the LADO are
- 0115 9773921 (County – non-schools)
  - 01623 433322 (County – schools)
  - 0115 8764718 (City)
- 2.9 Staff/volunteers should also be mindful that requirements in relation to maintaining the confidentiality of children and young people, their families, colleagues and the agency/organisation itself apply to all forms of communication, including that which takes place on social networking sites.

## 3. Indecent Images

### Child Abuse and the Adult

- 3.1 The viewing and possession of inappropriate and/or sexually graphic images and films of children is a form of child sexual abuse. There is some evidence that people found in possession of such images may be involved, either now or in the future, in the direct sexual abuse of children. When someone is discovered to have placed or accessed such material on the Internet, the Police should consider the potential likelihood that the individual is involved in the direct sexual abuse of children.
- 3.2 In particular, the individual's access to children should be established within the family, within employment contexts and in other settings such as voluntary work with children or other positions of trust.
- 3.3 Any indecent, obscene image involving a child has, by its very nature, involved a person, who in creating that image has been party to abusing that child.

### Children and Young People who are the Subject of Abusive Images

- 3.4 Children can be severely traumatised by knowing that images of them being abused exist on the internet and that these images will probably be subject to wide circulation. The situation is further compounded by the fact that different countries have different cultural perspectives regarding sexually provocative or indecent images of children and young people, which will be reflected in their legislation. Where this is the case, it can never be known if the image has been totally removed from the internet, and therefore in this sense the individual remains a victim, hence the need for specialised therapeutic support.

### Guidance upon the Discovery of Indecent Images of Children

- 3.5 It is a criminal act under Section 1 of the Protection of Children Act 1978 and Section 160 of the Criminal Justice Act 1988 for any person to make, distribute and/or possess indecent images of children. There are additional offences in respect of child pornography under the Sexual Offences Act 2003. These are all arrestable offences.
- 3.6 Upon the receipt of any information concerning a person or persons suspected of this kind of activity, the appropriate manager within the agency should notify the Police immediately. No downloading or distribution of any

images should be completed, either internally or externally within the agency, as this will leave the individuals responsible also open to criminal investigation.

- 3.7 If the computer or device belongs to the agency, it should be left and not used by anyone, allowing this to be seized as evidence for forensic examination by the Police. The details of all persons having access to the computer should be made available to allow a clear evidence trail to be established.

### **Actions to be taken where an Employee has Concerns about a Colleague accessing indecent images.**

- 3.8 Where an employee has either information or reason to suspect that a colleague is accessing indecent images of children, the following steps must be followed:

- the employee with the concerns must inform his/her own line manager the same working day
- where the concerns are about the line manager, then the employee should go straight to the next in line senior manager, or any other senior manager, within the same working day
- the manager who receives the information should ensure the computer in question is appropriately secured, and that it is not used by any other employee.

- 3.9 Where an employee does not feel confident in informing any available line manager, then the agency's own whistle-blowing procedures should be used.

- 3.10 The line manager should consider the Allegations Management procedures within the NCSCB / NSCB Safeguarding Children Procedures and contact the LADO where appropriate.

- 3.11 Where there is suspected or actual evidence of anyone accessing or creating indecent images of children, this must be referred to the Police and Children's Social Care.

- 3.12 Due to the nature of this type of abuse and the possibility of the destruction of evidence, the referrer should first discuss their concerns with the Police and Children's Social Care before raising the matter with the family. This will enable a joint decision to be made about informing the family and ensuring that the child's welfare is safeguarded.

- 3.13 All such reports should be taken seriously. Referrals will be followed by an Initial Assessment and information should be shared between the Police and Children's Social Care by way of a Strategy Discussion.

- 3.14 A Strategy Discussion and any Section 47 Enquiry and Core Assessment must carefully consider:

- Is there a child at immediate risk of Significant Harm e.g. the child in the image or a child in the household?
- What is the impact on the child in the image/in the household in terms of risks and their needs?
- Are there other children visiting the household? What is the impact on them?
- Is the person accessing images or creating them, in contact with children in their workplace?
- Is the person accessing or creating images involved in voluntary work, youth work or any other activity involving positions of trust?
- What is the timescale for a forensic investigation of any computer equipment?
- If the person is to be investigated, how should their contact with children be managed in the meantime, in the workplace and/or at home?
- Is the other parent or any other carer in the household able to protect the child? What support networks do they have?
- What are the implications of the likely delay in the criminal investigations?

3.15 Intervention should be continually under review if further evidence comes to light.

### **Outcome of the Section 47 Enquiry**

- 3.16 Where the enquiries have revealed that there are children in the household or in regular contact with the household about whom there are concerns of continuing risk of Significant Harm, an Initial Child Protection Conference must be convened within 15 working days of the last Strategy Discussion.
- 3.17 Where there are no children identified as at continuing risk of significant harm in relation to the adult, the Police will continue with investigations in order to establish the identity of the child/ren in the images if at all possible. The National Police Child Abuse and Internet Specialist Services will be informed as appropriate.
- 3.18 Where there are no children identified in the adult's household or immediate home environment but the adult is in contact with children in other settings such as work or other activities, the Allegations Management Procedure should be followed (chapter 7 of the interagency NSCB/NSCB procedures).
- 3.19 Where the person, who is alleged to have accessed or created the indecent images, is a child, action should be taken in accordance with arrangements for responding to concerns regarding children who may be displaying sexually harmful behaviour. In the City this process is the assessment and early intervention (AEIP) model. In the county the Assessment, Intervention Moving on (AIM) model.

## 4. Cyber Bullying

- 4.1 Cyber bullying can be defined as 'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset and intimidate someone else'. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, and even the profile of the person doing the bullying and their target. Research into the extent of cyber bullying indicates that it is a feature of many young people's lives. It also affects members of staff and other adults.
- 4.2 Cyber bullying takes different forms: threats and intimidation, harassment or 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images (for example, images that have been misleadingly referred to as 'happy slapping'), and manipulation.
- 4.3 Some cyber bullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyber bullying are known to be unintentional and the result of simply not thinking about the consequences. What may be sent as a joke may not be received as one, and indeed the distance that technology allows in communication, means that the sender may not see the impact of the message on the receiver. There is also less opportunity for either party to resolve any misunderstanding or to feel empathy. It is important that children and young are made aware of the effects of their actions.
- 4.4 Essential elements of prevention are awareness raising and promoting understanding about cyber bullying through discussion and activity around what it is, and how it differs from other forms of bullying.
- 4.5 For those agencies working directly with children and young people it is important to review and update existing anti-bullying, behaviour and pastoral-care policies to include cyber bullying. These agencies should ensure that children and young people, parents/carers and staff are all aware of the procedures and sanctions for dealing with cyber bullying, including bullying that takes place out of the setting.

## 5. Glossary of Current Legislation

### Computer Misuse Act 1990

5.1 The Computer Misuse Act makes it an offence for anyone to have:

- Unauthorised access to computer material e.g. if you access someone else's email account without their permission.
- Unauthorised access with an intention to commit further offences e.g. If you access someone else's email account with the intention of committing a fraud.
- Unauthorised modification of computer material e.g. If you change data without permission on a computer or intentionally introduce a virus that affects its performance.

### Protection from Harassment Act 1997

5.2 The most important elements of the Act include:

5.3 **Section 2** – A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

5.4 **Section 4** – A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions

### 5.5 Communications Act 2003

5.6 There are 2 separate offences under this act:

- (a) sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
- (b) sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

5.7 This wording is important because the offence under (a) is complete when the message has been sent – no need to prove any intent or purpose. It is an offence under (b) to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.

## **Malicious Communications Act 1988**

- 5.8 Offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.

## **Public Order Act 1986**

- 5.9 Offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

## **Obscene Publications Act 1959 and 1964**

- 5.10 Defines “obscene” and related offences.

## **Copyright, Design and Patents Act 1988**

- 5.11 It is an offence to use unlicensed software

## **Protection of Children Act 1978**

- 5.12 The law on images of child abuse is clear. It is an offence to possess indecent images of children in the United Kingdom.

## **Sexual Offences Act 2003**

- Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
- Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (Note: to view an indecent image on your computer means that you have made a digital image.)
- Causing a child under 16 to watch a sexual act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
- Abuse of positions of trust – Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust (it applies to teachers, social workers, health professionals, Connexions staff etc).
- Causing or inciting a child to engage in sexual activity
- Engaging in sexual activity in the presence of a child under 16
- Exposure

## Sex Offences Act 2003 Memorandum of Understanding

- 5.13 Memorandum of Understanding between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.
- 5.14 The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum has been created within the context of child protection, which will always take primacy.
- 5.15 The MOU: <http://www.iwf.org.uk/hotline/the-laws/child-sexual-abuse-content/sexual-offences-act-2003-memorandum-of-understanding>

## The Data Protection Act 1998

- 5.16 Gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.
- 5.17 The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act can be summed up in 8 principles, which must be satisfied when processing personal data (information that will identify an individual). The Act also gives rights to the people the information is about and allows individuals to find out what information is held about them.
- 5.18 The eight principles are that personal data must be:
- Processed fairly and lawfully
  - Personal information must be processed for specified purposes
  - The information held must be adequate, relevant and not excessive
  - The information must be accurate and up-to-date
  - The information should not be held no longer than is necessary
  - The information should be processed in line with individuals rights
  - The information must be kept secure
  - The information should only be transferred only to other countries with suitable security measures.