All Wales Child Protection Procedures Review Group

Grwp Adolygu Canllawiau Amddiffyn Plant Cymru Gyfan

The Protection of Children and Young People at risk or experiencing harm through the use of Information Communication Technology (ICT)

All Wales Protocol

FINAL	July 2015
Implementation	December 2015
Review	

5.5.1 Introduction

This guidance is intended to inform professionals working with the protection of children and young people who may be at risk of or experiencing abuse via information communication technology. This is not guidance to advise on E Safety for children or young people, carers, parents or professionals (see 5.5.7 below for helpful resources in this area) nor is it guidance for professional behaviour in the use of Information Communication Technology, as this is a matter for an employing organisation and/or professional codes of conduct.

5.5.2 Definition of Information Communication Technology (ICT)

For the purposes of this guidance information communication technology refers to all forms of social communication that take place through the use of electronic equipment. Such equipment currently includes mobile phones, computers, games consoles and tablets, but other types of equipment may develop in the future. Because the forms of this type of technology and the forms of communication it enables are developing, information communication technology or ICT is used as a 'catch all' category for ease of reference.

5.5.3 Forms and Specific Risks of Child Abuse via ICT

The main forms of Child Abuse via ICT

For the purposes of this guidance the main forms of child abuse via ICT; **Content**, **Contact** and **Conduct**; have been drawn from the Byron Review (2010) and Advice on Child Internet Safety 1.0 (2013).

- **Content**: This refers to harm through exposure to images, text and audio that are age inappropriate, offensive or illegal. Examples include adult pornography, images of extreme violence and sadism and images of sexually abused children. A case example is a Health Visitor observing pornographic images on a family computer that young children in the household can see.

- **Contact**: This refers to harm through interactions with others. Examples include on-line grooming for sexual abuse and exploitation, children being sexually abused to create images for self-gratification or sharing with others: and vulnerable adults with children targeted by abusive adults via dating websites so as to access their children. It can also include 'secret' contact between children looked after by the local authority and family members or others, where such contact has been prevented by professionals to protect the child from harm.

- **Conduct**: This refers to harm arising from how children and young people behave when communicating between themselves or with adults using ICT. Examples include 'cyber' bullying and 'cyber' stalking, such as a young person telling their

social worker that they are being threatened via text messages to their phone and abusive comments on Facebook. A further example is children and young people exchanging sexual images and messages ('sexting').

Specific Risks

- **Virtual Identities**

Individuals have greater control over how they present themselves to others and greater opportunity to create new identities through which to engage with children, young people and their carers and parents. For example, adults can pose as children or young people as a grooming strategy through social media such as 'chat rooms'. In addition adults can start new relationships on the basis of little knowledge of each other. Again this can be a grooming strategy through which abusive adults can access children and young people.

- **Unsupervised Contact**

Children and young people can contact and be contacted by others and access the internet through a range of means such as mobile phones, game consoles and tablets. In addition they are able to do this by using other people's equipment, such as friends, even though safeguards such as parental controls etc. have been put in place on their own equipment. Therefore parents, carers and professionals may often have minimal knowledge, if any, of a child and young person's ICT usage, who they are in contact with, the relationships they have and if they are acting in a safe way.

For children and young people who are looked after and whose contact with birth parents or others is supervised for their own protection, this can be undermined by 'secret' communication through access to ICT and social networking sites. Risks that have been identified with unsupervised contact are physical and sexual harm through meeting up, disclosure of location, disruption of placements and emotional harm arising from such contacts.

Unsupervised contact can prevent carers and parents, professionals and others being aware of the risk or actual abuse and then intervening and reporting concerns.

- **Online communities**

Communication via ICT increases the opportunities and means for those seeking to abuse children and young people. This is because it is possible to locate, contact and build up relationships with children, young people and/or their parents and carers through various social media or common interest sites. Equally it enables people who have a sexual interest in children to communicate with each other.

This risk is highlighted in 'The Independent Inquiry into Child Sexual Exploitation in Rotherham (2014);
'A number of the recent case files we read demonstrated that by unguarded use of text and video messaging and social networking sites, children had unwittingly placed

themselves in a position where they could be targeted, sometimes in a matter of days or hours, by sexual predators from all over the world.' (p.44).

Through such networks of contacts sexually abusive behaviour can become normalised and encouraged. One outcome of this is that vulnerable adults, with access to children, and a tendency towards abusive behaviour, can be groomed to sexually abuse children and share images with others.

- **Ease of sharing information**

Images, text and audio can be easily shared once sent or posted on line leading to the sender losing control of how these are used, shared, in what form and with whom. This is a particular issue for self-generated pictures taken by children and young people.

(Learning from case reviews where online abuse was a key factor - NSPCC briefing (taken from NSPCC Library thematic review 21/7/14)

- **Violent Extremism**

ICT is being utilised by groups or individuals who span a spectrum of beliefs and are committed to violent extremism to recruit children and young people to participate in or support their activities. Examples of the methods used include videos, Podcasts and websites. The use of social media and the internet by extremist groups to target vulnerable young people for recruitment to violent extremist causes has been clearly identified by the UK government. The Prevent Review (2011) noted that the internet and social media had 'transformed the extent to which terrorist organisations and their sympathisers can radicalise people in this country'.

The Crown Prosecution Service define violent extremism as "The demonstration of unacceptable behaviour by using any means or medium to express views, which:

- Encourage, justify or glorify terrorist violence in furtherance of particular beliefs;
- Seek to provoke others to terrorist acts;
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts;
- Foster hatred which might lead to inter-community violence in the UK."

Once referred to Social Services or reported to the Police the child protection process must include a referral to the area Single Point of Contact (SPOC) for the Prevent Programme or the Channel Programme. The SPOC for both Prevent and Channel is held by the Police.

5.5.4 Principle Offences

There are a number of offences that relate to child abuse via ICT that fall under the 'Contact', 'Content' and 'Conduct' categories. Because these offences are numerous and can change over time professionals are advised to liaise with the Police or Crown

Prosecution Service for information in this area. For guidance as to the categorisation of sexual abuse images see Sentencing Council Sexual Offences Definitive Guideline

5.5.5 Management of Child Protection Cases

Some professionals may be concerned through a lack of familiarity with the ICT world that the management of child protection is very different, this is the not the case. The management of child protection cases involving ICT follows the same process and procedures that need to be followed for child protection concerns (see **Part 3** of the main **All Wales Child Protection Procedures 'The Child Protection Process'**). Therefore concerns regarding children at risk or experiencing abuse via ICT should be reported/referred to Social Services and the Police immediately and managed through the child protection process (see **Part 3** of the main **All Wales Child Protection Procedures 'The Child Protection Process'**).

Additional considerations for Professionals are that they should be aware that cases of online abuse are rarely confined to a single victim and perpetrator. Therefore such cases should be considered as potentially complex and managed on the basis that there is a possibility that there are other victims and abusers. In addition, where a case of online grooming is identified, as well as reporting and referring to Social Services and the Police in the first instance, further reports may be made to both the **Child Exploitation and Online Protection Centre (CEOP)** and/either the **Internet Watch Foundation (IWF)** or the internet site through which the grooming took place. This should only be done after the concern has first been referred/reported to Social Services and/or the Police.

5.5.6 Preservation of Evidence

Evidence can be critical in identifying other children who have been abused and other perpetrators and the Police are the lead agency for gathering such forensic evidence. Professionals should note that evidence of abuse via ICT is often, but not always, contained on the equipment itself and that images and text that has been deleted may be retrieved by trained forensic examiners. It is also important to note that due to the design of some devices and software that access to evidence may not be possible without the cooperation of the victim to produce and secure evidence, especially with 'off line' offending.

The ACPO guidance in this area is that:-
"Officers should take care to seize any device in accordance with the principles of the ACPO Good Practice Guide to Forensic Computing, which requires that no data held on a computer at the time of seizure should be altered or compromised in any way. In plain language, nothing should be switched on, viewed, deleted or in any way manipulated prior to forensic examination by the police. "

In addition that;

‘Digital devices and media should not be seized just because they are there. The person in charge should have reasonable grounds to remove the property and there should be justifiable reasons for doing so……’

(ACPO Good Practice Guide for Digital Evidence version 5 October 2011)

Recovering forensic data from ICT equipment is a specialised activity and therefore must always be left to the Police, therefore other than securing what evidence is in the professionals procession in both ‘hard’ and electronic form, no attempt should be made to access the evidence.

To ensure the integrity of the forensic evidence ‘chain’ for the Police, professionals are advised to report concerns to CEOP and/or the Internet Watch Foundation only **after first reporting** to Social Services or the Police, who may refer to these agencies themselves.

5.5.7 Specialist Reporting (CEOP) and Resources

It should be noted that all referrals and reports must first be made to Social Services and the Police. A main specialist resource for professionals is the Child Exploitation and Online Protection Centre (see hyperlink to above) which is a UK wide child protection law enforcement command of the National Crime Agency. In addition to its law enforcement activities CEOP also provides advice and training for professionals and information and reporting for the general public, including children and young people. Reporting can also be made to the Internet Watch Foundation (IWF) which is an independent self-regulated organisation which works;

‘in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of potentially criminal child sexual abuse content hosted anywhere in the world, criminally obscene adult content hosted in the UK and non-photographic child sexual abuse images hosted in the UK.’

The remit of the IWF is ‘to minimise the availability of potentially criminal internet content specifically:

- Child sexual abuse content hosted anywhere in the world.
- Criminally obscene adult content hosted in the UK.
- Non-photographic child sexual abuse images hosted in the UK’

(IWF 18/09/2014)

Other sources of information to guide professionals with ICT safety and behaviour for children, young people, cares and parents and professionals are:-

Thinkuknow – Information for 5-7, 8-10, 11-13, 14+, Parents & Carers, Teacher Training https://www.thinkuknow.co.uk/

Child Net – Internet safety guides & tips for parents, carers, young people and professionals http://www.childnet.com/

Child Net - Internet safety Hot Topics
http://www.childnet.com/teachers-and-professionals/for-working-with-young-people/hot-topics

Newsround - Special report on internet safety
http://www.bbc.co.uk/newsround/13908828

Internet matters – expert advice, guides and top tips on staying safe online
http://www.internetmatters.org/

Kidsmart – interactive site providing lots of ideas on internet safety
http://www.kidsmart.org.uk/

NSPCC - Advice for parents about keeping your child safe when using the internet, social networking websites and online gaming
http://www.nspcc.org.uk/help-and-advice/for-parents/online-safety/online-safety_wdh99554.html

CEOP (Child Exploitation and Online Protection Centre) – advice, help and report centre
http://ceop.police.uk/safety-centre/

Childline - Information on dealing with Online bullying
http://www.childline.org.uk/Explore/Bullying/Pages/online-bullying.aspx

Wise Kids - Online Safety Tips for Children and Young People
http://wisekids.org.uk/wk/

Get Safeonline – free expert advice on safeguarding children
https://www.getsafeonline.org/safeguarding-children/

Please note that the subject of internet safety and safety with technology covers a very broad range of topics with many topic related websites and webpages that may not always be age appropriate.

5.5.7 Glossary

Although certain terms such as ‘sexting’ and ‘cyberbullying’ have been used in this procedure the nature of the ICT world is such that that it is developing and dynamic, which means that the terminology can become out of date relatively quickly. Therefore professionals are guided to the resources above for current glossaries.