Chapter P: E-Safety Policy and Guidelines

SCOPE OF THIS CHAPTER

This guidance has been written in conjunction with and is endorsed by Peterborough Safeguarding Children Board. It aims to consolidate advice for all professionals working with children, advice for parents and children on keeping children and young people safe in a modern world.

Modern information and communication technology has developed rapidly in recent years and continues to do so at an unprecedented pace. No guidance can hope to keep up with future developments. However PCC hopes that this document will act as a central reference point and it will be regularly reviewed and updated.

This guidance is relevant across the children's workforce and to those responsible for children and young people's welfare in these settings

The educational and social benefits of Information Communication Technology (ICT) are widely recognised but are unfortunately accompanied by some risks which although not eradicated can be minimised by a number of safe practice recommendations and enable children and young people to be safe and discriminating users

RELATED GUIDANCE

Please see **ACPO Briefing on Young People who Post Self-Taken Indecent Images**.

AMENDMENTS

Section 3, Guidance for Parents and Carers of this chapter was amended in November 2009 to the effect that the information from the Child Exploitation Online Protection Service is now that 1 in 4 children and young people (rather than 1 in 12) have met offline someone they met online.

A link to the ACPO guidance on Self-taken images was added in June 2011.

Contents

1. Guidance for Children and Young People

Top Tips for Staying Safe

- Remember everyone you meet online is a stranger even if they might seem like a friend
- Always use a nickname when you log on and **never** give out any personal details that would allow someone you meet on line to contact you.

  This means full name, home or school address, telephone or mobile number or personal email. It also includes not saying your favourite places to eat or play sport
- Never arrange to meet alone someone you make friends with online. They may not be who they say they are. If you are going anyway take an adult you trust and meet in a public place
- Try to have your own online conversations in public. People are less likely to hassle you if other people can see you doing it
- Accepting emails or opening files from people you don't really know can get you into trouble – they may contain viruses, nasty messages or annoying links to stuff you don't want to see
- Talk to an adult you know well and ask for help if you're worried or upset about anything you've seen or been sent online
- You can also directly report any unsuitable material or behaviour to the child exploitation online protection service or the internet watch foundation – see section 7

2. Guidance for Schools, Libraries, After School Clubs, Youth Clubs and other Establishments

All establishments are recommended to rigorously adopt these recommendations in order to minimise any risks to children and young people through the use of the internet and other ICT

2.1 Important principles

- There must be an agreed principle that all staff, volunteers and students recognise their responsibilities with regard to internet safety
- Everyone needs to have clear guidance about how facilities can and cannot be used by young people, professionals and volunteers and what sanctions will be used if misuse occurs
- A comprehensive internet safety programme should be included in the curriculum for the whole school community and where possible an appropriate programme for other settings developed

- Each school should have a designated internet safety coordinator who will assist with developing the school acceptable use policy and other settings should have a co-ordinator to develop a policy for their setting.

2.2 Internet use - receiving information

All schools/establishments should be using a filtered internet feed from an education accredited internet service provider

It is vital that staff recognise that filters can only reduce and not eliminate access to inappropriate material. Staff should be mindful of their responsibilities for supervising children and consider carefully the position of monitors in order to facilitate this.

Children and young people should be given clear instructions on how to report any inappropriate or offensive material

Students, especially younger students, should be encouraged to use search tools such as Yahooligans which search across a restricted range of websites with educational relevance

In addition all schools/establishments should use a monitoring mechanism which will enable unsuitable or inappropriate material to be detected and recorded for further action

Learning to use the internet safely and appropriately is an important part of pupils' education and should be incorporated into the curriculum throughout the school

Children and young people should be taught to check with their teacher/youth leader before providing any personal information that may be requested by a specific website. They should understand that they should only supply minimal untraceable details, such as a first name, to an enquiring website and should never divulge anyone else's personal information.

2.3 Internet use – publishing information

The disclosure of personal information on the internet poses the most serious risk that a child or young person could be hurt exploited or abused. It is crucial that children and young people do not reveal any personal details which could result in their being traced. Such details include full name, home or school address, telephone or mobile number or personal email address. It also includes age, gender and information about likes and dislikes and favourite places as all of this can be used for tracing and contact purposes

Any risk to children may not be immediate as potential abusers may be content to spend a long period of time building up a relationship. This is known as grooming and constitutes a crime

An adult over the age of 18 who has communicated with a child under the age of 16 at least twice including by phone or internet will be committing an offence if they meet them or travel to meet them anywhere in the world with the intention of committing or engaging in sexual activity (under the Sexual Offences Act 2003).

The names (first or surnames) should never be attached to photos on websites - see **Section 6, Use of Images** for further guidance.

2.4 Access and the Safe Use of IT equipment - Guarding against IT misuse

There have been occasions when IT equipment has been misused and inappropriate material has been accessed. The following guidance has been written in order to minimise such opportunities and also to advise on appropriate action if there is a suspicion that such misuse has occurred.

1. All schools and other organisations are advised to secure their PC's and network from unauthorised access. This can be done in a number of ways
2. All PC's should be configured so as to present an authentication challenge on start up. This can be simplified in order to enable access by younger children
3. PC's and servers should be configured to present a screen lock and authentication challenge after a period of inactivity. This is essential for any PC's or servers that are left on all the time.
4. **All users of IT including all staff, children and volunteers should be issued with their own unique user id and password to ensure there is accountability and an audit trail of their activities. Problems for younger children in logging on can be resolved with the use of biometrics/**
5. **All staff, volunteers, children and young people should be instructed to never divulge their passwords to anyone.**
6. A person specifically named in the organisation's IT policy should monitor any potential problems in their organisation using an appropriate monitoring system which provides monthly reports and additional alerts if there are attempts to access inappropriate material.
7. Each organisation's filter log should be analysed for evidence of child sex abuser key words. A report should identify date and time of any blocks together with the unique user id
8. All organisations should issue an IT security policy which includes a section on acceptable email and internet usage. This policy should apply to all students, volunteers and staff alike
9. Staff and volunteers should sign a declaration that they have read, understood and will comply with this policy before being given access to IT equipment. This should also be a requirement for any external users
10. Organisations should ensure that only those with a genuine need to access systems are provided with user ids

2.5 Action if misuse is suspected

Staff should trust their judgement and quarantine the PC without undertaking any investigations of their own

The following procedure should be observed

- the police should be contacted immediately

- if effective monitoring is in place the evidence will be in a sealed box
- arrangements will be made to collect the evidence for forensic examination

Organisations should never attempt to access a site which they believe to be illegal – to do so would break the law and make them liable to prosecution

If there is any doubt about the subject matter, it is enough to view the internet history. Any attempt to follow the internet hyperlinks to the sites themselves will invalidate evidence by updating the time stamps of images received

The police should be contacted if there are concerns or suspicions about access to child sex abuse images or any other illegal material

3. Guidance for Parents and Carers

The Child Exploitation Online Protection Service has recently revealed that 1 in 4 children and young people have met offline someone they met online.

Parents are advised to:

- Regularly remind children and young people of the dangers of disclosing personal information and that people they meet online are not necessarily who they seem
- Keep the computer in a communal area such as a family room where you can keep an eye on what the child or young person is accessing on the internet
- Use an appropriate filtering system to minimise opportunities to access unsuitable material. Contact mobile phone service providers to discuss how you can limit access to inappropriate internet sites e.g. pornography or gambling websites
- Talk to your child about their internet use and let them know you are there to discuss anything of concern. Do not overreact if they do bring something to your attention. Your involvement is the best way of keeping them safe
- Do not feel intimidated by your lack of technical knowledge – take advice if you need additional expertise - see **Section 7, Sources of Further Information**

4. Cyber Bullying

Cyber bullying is when one person or a group of people aim to threaten, tease or embarrass someone else by using a mobile phone, the internet or other technologies. Even though cyber bullying cannot physically hurt someone, it can still leave the victim feeling mentally vulnerable and very upset. They can also feel scared, lonely and stressed and that there's no way out.

Escaping cyber bullying can be very difficult. Because anyone can get access to a mobile phone or the internet almost anywhere, it can even be tough for those on the receiving end to avoid it, even in the safety of their own home.

Even though those that use the web to target and bully others think that they can remain anonymous, this isn't the case. Even someone using a false name or email address can be traced and banned by social networks and email providers if they're found to be bullying others.

Don't be tempted to take on the person who's carrying out the bullying yourself by responding to them in a way that's just as threatening. You may become guilty of bullying yourself, or make yourself another target for someone to threaten.

If you do notice bullying taking place on instant messenger, in a chat room or on a social networking site, report it to the website administrators or internet service provider. You should be able to do this easily through the site itself.

If you notice bullying happening on a mobile phone, contact your mobile service provider.

If you encounter any other forms of cyber bullying, especially those that use racism, religious hate, homophobia or threats of actual violence, tell your parents, a teacher or – if you think that the content is illegal – the police.

Other ways of dealing with cyber bullying

- talk to someone you trust about it, like a friend, a teacher or an older relative or call a helpline such as Childline 0800 1111
- keep and save any bullying emails, text messages or images you receive as they can be used as evidence
- make a note of the time and date that messages or images were sent, along with any details you have about the sender
- try changing your online user ID or nickname
- change your mobile phone number and only give it out to close friends
- mobile phone companies and internet service providers can trace bullies, so don't be afraid of reporting it to them
- block instant messages from certain people or use mail filters to block emails from specific email addresses
- don't reply to bullying or threatening text messages or emails – this could make matters worse and lets those carrying out the bullying know that they've found a 'live' phone number or email address
- report serious bullying, like threats of a physical or sexual nature, to the police

Schools may still be able to take action about cyber bullying even it is happening out of school. The Education and Inspections Act 2006 gives head teachers the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are offsite

5. Mobile Phones

The above internet guidance applies equally when a mobile phone rather than a PC is used to access the internet. Schools can adopt the following model mobile phone policy in order to minimise misuse. Other settings can modify this for their own use.

Model School Policy on the Use of Mobile Phones

XXXX school recognises that parents may wish their children to have mobile phones for use in cases of emergency. However mobiles can be used inappropriately, and are potentially targets for theft and the Governing Body has therefore adopted the following policy, which will be rigorously enforced

- As there is no legitimate use for mobiles on school premises, students may not use them for any purpose whilst on the school premises and must keep them out of sight at all times
- Students who ignore this policy and use a mobile on school premises will be required to hand over their phone to a member of staff. Parents will be contacted to inform them that this has happened and asked to collect it from the school office.
- If a member of the staff of the school has any suspicion that a mobile phone has unsuitable material stored on it students will be required to hand over the phone to a member of staff and parents will be asked to collect it from a senior member of staff. In circumstances where there is a suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Parents will need to recover the phone from the police in such circumstances
- Students remain responsible for their own property and will bear the responsibility of any losses
- Any failure to comply with the above guidelines may result in normal disciplinary action to be taken up to and including the consideration of permanent exclusion of the student concerned
- Parents should be aware that whilst there are obvious benefits to students having mobiles in terms of personal safety there are also some associated risks such as potential for theft, bullying and inappropriate contact, including grooming by unsuitable persons.

See also **Appendix C, Advice on Safe Use of Mobiles** – Guidelines for parents and students on safe use of mobile phones

6. Guidance for Schools on the use of Images

For ease of reference the term ‘images’ includes photographs and video images using digital and non digital cameras, mobile phones and webcams.

6.1 Introduction

Schools, other educational organisations and establishments are advised to have a clear policy which outlines the safety guidelines for the use of photography and other images of children and young people.

The use of images can be divided into three broad categories:

- Images taken by staff for education and publicity purposes
- Images taken by parents at school events
- Images taken by third parties

6.2 Images taken by school

The Data Protection Act 1998 affects the use of photography. An image of a child is personal data and it is, therefore a requirement under the Act that consent is obtained from the parent of a child for any images made such as those used for school web sites, productions or other purposes. It is also important to take into account the wishes of the child, remembering that some children do not wish to have their photograph taken.

A signed consent form should be obtained from the child's parent/carer, and should be kept on the child's file, covering all cases where images of children are to be used. For an example of consent form see **Appendix B, Use of Images Consent Form**. This could be an addition to the school's admission form. Parents may withdraw consent at any stage, but they would need to do so in writing.

Images must be maintained securely for authorised school use only, and disposed of either by return to the child, parents, or destroying as appropriate.

Care should be taken in relation to particularly vulnerable children such as those who are in public care, recently adopted or those resettled following on from domestic abuse

6.3 Parents wishing to take images at school events

Increasingly technology is making it easier for images to be misused and it is therefore important that organisations take practical steps to ensure that images of children taken by parents and carers and by members of the media are done in a way that is in accordance with its protective ethos.

The Data Protection Act does not prevent parents from taking images at school events, but these must be **for their own personal use**. Any other use would require the consent of the parents of other children in the image.

The manager of the organisation or head teacher in consultation with governors should agree when parents are to be permitted to take images. This information could be included in invitation letters to parents.

Parents should be required to give an undertaking on how the images will be used – see **Appendix A, Parents' form of Undertaking.**

Parents should also be advised that they may only take images in designated circumstances and areas such as in the school hall and not backstage or in changing rooms. It is important that parents understand their responsibilities for the safekeeping of any images they may take.

Consideration should be given to a special photo call session at the end of the event – this would avoid distraction and disturbance and also allow for the withdrawal of children whose parents/carers have not consented.

It is recommended that wherever possible schools take their own 'official' photos or videos in order to retain control over the images produced.

It is also important to ensure that people with no connection with your school do not have any opportunity to produce images covertly. Staff should question anyone who is using a camera or video recorder at events they do not recognise.

6.4 Publishing or displaying photographs or other images of children

The Department for Children Schools and Families advise the following,

- If the pupil is named, avoid using the photograph.
- If the photograph is used, avoid naming the pupil.

Whatever the purpose of displaying or publishing images of children care should always be taken to avoid the possibility that people outside the organisation could identify and then attempt to contact children directly. Most abused children are abused by someone they know, but there is still a concern that children might be identified from pictures appearing in the press or other media and targeted for abuse.

- Where possible, general shots of classrooms or group activities rather than close up pictures of individual children should be used. The camera angles should be considered. Photographs taken over the shoulder, or from behind are less identifiable.
- Children should be in suitable dress, and images of PE or swimming events should maintain modesty, for example wearing team tracksuits if appropriate
- Children from different ethnic backgrounds should be included in your communications wherever possible, as well as positive images of children with disabilities to promote the school as an inclusive community, and to comply with the Disability Discrimination Act
- Children can be identified by logos or emblems on sweatshirts etc. Depending on the use to which the photograph will be put, airbrushing logos should be considered.
- An article could be illustrated by the children's work as an alternative to using an image of the child

It is essential that when considering inviting an official photographer schools establish the validity of the organisation and what checks/vetting has been undertaken. Procedures should also ensure that levels of supervision are appropriate to safeguard the welfare of children at all times when visitors are present on the school site.

There may be occasions where the media take photographs at your school of pupils. It is important that parents and carers are aware of the potential risks and benefits so they can make an informed decision about consent.

If a child is photographed by a newspaper, the photo becomes the property of the newspaper and the newspaper has the final say as to how it is used. (N.B. images can be placed by editors on the newspaper's website). Generally, newspaper photos of groups of 12+ children do not have the names of the children attached. However, photos of groups of less than 12 children are likely to include the full name of the child in the accompanying caption. Parents need to be aware when they give consent that this is the position. It is important that they are also reminded of the benefits of publicly celebrating achievement to build esteem in the child and pride in their school.

6.5 Websites and Web cams

Consent gained from parents/carers for the use of photographs or videos may not extend to website or web cam use, so it is important to check, when introducing such technology, the status of existing consent for children and young people.

It is important to take care with identification, and to respect parental views on the use of any photography of children on a website. See - see **Section 7, Sources of Further Information**

The regulations for using web cams are similar to those for CCTV (closed-circuit television). Children, their parents and other adults appearing on the web cam all need to be consulted and their consent obtained. In gaining consent, you must tell the person why the web cam is there, what you will use the images for, who might want to look at the pictures and what security measures are in place to protect access. In addition the area in which the web cam is being used must be well signposted so that people must know that the web cam is there before they enter the area.

The current DCSF advice (July 2003) is that unless a web cam is a response to a specific threat or difficulty in relation to either crime or health and safety it may pose more difficulties for the school than it would actually resolve. If a school wants to use a web cam, careful parental, staff and legal consultation is advised.

6.6 Using photographs of children supplied by a third party

Copyright of an image including those downloaded from the internet usually rests with the person who produced it

Before using an image supplied by a third party schools should check that the third party owns the copyright of that image and you should obtain their written permission to use it

Schools should ask a third party to guarantee to you that all relevant consents have been given and that they are entitled to provide you with the image.

7. Sources of Further Information

Kidsmart
Kidsmart website contains resources and activities including lesson plans quizzes and a parent's presentation
Child Exploitation Online Protection Centre
Child Exploitation Online Protection Centre website combines police powers with the business sectors – contains useful information on how to report incidents
Chat Danger
The Chatdanger website advice to children about chat related issues on the internet and on mobile phones
Safekids
The Safekids – family website includes internet contract for parents and children to sign
Think U Know
The Think u know website – staying safe on the internet - games and links to NSPCC Childline, Childnet and NCH
Internet Watch Foundation
Internet Watch Foundation website is the place to report illegal images
E2BN
E2BN website:The East of England Broadband Network (E2BN) is one of 10 Regional Broadband Consortia (RBCs) set up by the Government to help raise standards in teaching and learning by the use of broadband technology. Each RBC is formed from a group of Local Authorities (LAs) who work together with the aim of achieving better provision, value for money and performance for schools than could be achieved individually
Information Commission
The Information Commission website is the UK's independent authority set up to promote access to official information and to protect personal Information.
Teachernet - Safe to Learn
The Safe to learn website - embedding anti-bullying work in schools: includes advice on more specific types of bullying, such as "cyber-bullying" (either online or by email or mobile phone) and homophobic bullying.
Press Complaints Commission
Press Complaints Commission website

Abuse Nuisance and or Bullying Reporting Numbers

Mobile Phone Operators
O2 Nuisance Call Bureau Email: **ncb@o2.com** or 08705214000
Vodafone 191 from a Vodaphone phone or 08700700191
Orange call 450 on an Orange phone
T-mobile 150 on a T mobile phone
Social network/Instant Messaging Sites
Bebo – click on Report Abuse link below user's profile photo
Myspace – via the Contact Myspace link
Piczo – bottom of home page – contact us – report abuse
MSN – click help then report abuse
Yahoo – click help – then report abuse

Appendix A - Parents' Form of Undertaking

Request for Parents Wishing to Take their Own Photos/Videos

I agree to ensure that all images I take will be for my personal use, will be kept securely and be used appropriately
I agree not to distract or obscure the view of others whilst taking images

YES/NO

Signed.....
Relationship to child.....
Date.....
Thank you for your co-operation. The safe use of images can be a source of pleasure and pride and a valuable record of the achievements of your child

Appendix B - Use of Images Consent Form

XXXXXXXXX School

Use of Images Consent Form

During the year there may be some opportunities to publicise activities which may involve the use of an image of your child. This could be a photograph, video or website image
It is a requirement of the Data Protection Act 1998 that we have your consent to this.
We have adopted certain safeguards in order to minimise any risk to your child

- We will avoid the publication of your child's full name with any image on any of our material/website, etc.
- Only appropriate images will be taken - i.e. children will always be fully dressed and in designated areas
- Images will be kept securely and destroyed after their required time
- Any external photographer will have the validity of their organisation checked
- Appropriate levels of supervision will be undertaken at all times

Please note that we do not have control of how images taken by the media are published – see guidance for schools
Do you give consent to your child having images taken according to the above guidelines?

YES/NO

Signed.....
Relationship to child.....
Date.....

Appendix C - Advice on Safe Use of Mobiles

Advice on Safe Use of Mobiles	Guidelines for Students and Parents On the Use of Mobile Phones In School
Using your mobile can be great fun but you need to be careful and keep safe • Don't give out your number or friends' numbers to people you don't know, especially in Instant Messenger or Chat Rooms • Keep your security code or PIN number private • If you get texts, which upset you, don't reply but keep a record and tell an adult. In serious cases you can report it to the police • If you receive a rude or embarrassing image or text about someone don't forward it to others • Distributing sexual images of other young people is harassment and could be illegal. If you receive something like this tell an adult immediately • Ask permission before taking a picture of your friends and think before sending it on. Once sent you have lost control of it and it could become public before you know it See Kidsmart at www.childnet.int-org for more info on staying safe, leaflets and interactive games.	**School and City Council Logos** **August 2008**

Benefits	Potential Disadvantages	School Policy
• Students can use phones in cases of emergency • Students may	• Mobiles are valuable and can be lost or stolen • Students can	• Mobile phones should not be generally used on school premises and students should keep them switched off and out of sight. • In very unusual circumstances, such as

feel more confident knowing they can make contact with someone if in difficulties	be bullied by text messaging or silent phone calls • Mobiles can be used to communicate inappropriate material • Unsuitable people are known to use mobile phones and text messages to make inappropriate contact with young people.	a family emergency students should seek staff permission to use their phone • Any student ignoring this policy and using a mobile on school premises without permission will be required to hand over the phone to a member of staff and parents will be asked to collect it from the school office. • If a member of the staff of the school has any suspicion that a mobile phone has unsuitable material stored on it students will be required to hand over the phone to a member of staff. Parents will be informed and asked to collect it from a senior member of staff. In circumstances where there is a suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Parents will need to recover the phone from the police in such circumstances • Students remain responsible for their own property and will bear the responsibility of any losses • Any failure to comply with the above guidelines may result in disciplinary action being taken up to and including a consideration of permanent exclusion of the student concerned Thank you for your co-operation.

End