



**E-SAFETY:  
SAFEGUARDING  
CHILDREN AND  
YOUNG PEOPLE  
USING  
DIGITAL AND INTERACTIVE  
TECHNOLOGY**

**May 2009**

<b>Title of Protocol</b>	<b>E-Safety: Safeguarding Children and Young People Using Digital and Interactive Technology</b>	
<b>Application</b>	<b>All BSCB partner agencies</b>	
<b>Date of initial ratification</b>	<b>May 2009</b>	
<b>Date of next review</b>	<b>May 2010</b>	
<b>Section</b>	<b>Contents</b>	<b>Page No.</b>
1.0	Introduction	3
2.0	Purpose	3
3.0	Aims	3
4.0	Definition	4
5.0	Categories of Risk	5
6.0	Minimising Risk	7
7.0	Procedures for Reporting Concerns	8
8.0	References	9
Appendix 1	Acceptable Use Policies	10
Appendix 2	Assessing Risk and Identifying Problems for Children and Young People	30
Appendix 3	Indicators of Risk of Sexual Exploitation via Digital and Interactive Technology	31
Appendix 4	Offences related to Digital and Interactive Technology	32
Appendix 5	How to Work Safely with Information and Communication Technology	36
Appendix 6	Guidance for Professionals to Minimise the Risk of Misconduct Allegations related to Digital and Interactive Technology	38

## Introduction

1.0 The development and now widespread use of the Internet, mobile phone and gaming technology has significantly enhanced our ability to communicate, entertain and learn. There are enormous benefits to using such digital and interactive technology, and as a result its use is widespread in schools, other educational settings including youth clubs, libraries, cafes, and hotels, as well as in the home. The Government's Home Access programme, which intends that every child aged between 5 and 18 will have home Internet access by 2013, highlights their belief in the importance of such a tool for education and development.

1.1 However, there are risks to all of us who use digital and interactive technology and we have a responsibility, therefore, to safeguard and promote the welfare of children and young people and help them develop the skills to look after themselves. We also have a responsibility to take action against those who harm children and young people via digital technology.

1.2 Much work has already been done in schools, with teachers, pupils, and to a lesser extent - parents, to raise awareness of the risks associated with using digital technology. The challenge for us now is to roll this out to the wider community, whilst at the same time keeping abreast of new technological developments. This is particularly important when the majority of children and young people often have more experience and confidence in using such technologies than their parents or other responsible adults.

1.3 This protocol is about safeguarding children and young people in a digital world. However, due to the vulnerability of some adult professionals to being cyberbullied, **Appendix 6**, provides guidance to professionals to better be able to safeguard themselves.

## Purpose

2.0 The effects of abuse suffered by children and young people via digital technology are the same as that which occurs via personal contact. Indeed, some physical and sexual abuse may occur as a result of initiation via digital technology. However, the impact may be more severe in some cases as the abuse via digital technology can take place in the home, where a child or young person should feel safe. Therefore it is **the responsibility of all professionals to ensure they know what to do if they suspect a child or young person is involved, or at risk of involvement, either as a victim or perpetrator, of abuse via digital technology**. The purpose of this protocol is, therefore, to provide guidance to all those working with children, young people and their families in Barnsley.

## Aims

3.0 The aims of this protocol are as follows:

- to define the different types of digital technology and the risks they present to children and young people

- to provide guidance to professionals regarding the safeguards that should be in place to protect children and young people using digital technology, whatever the setting
- to provide information about assessing a child or young person's level of risk, and some risk indicators, through their use of digital and interactive technology
- to provide guidance to professionals as to what action they should take if they are concerned about a child or young person related to digital and interactive technology, and provide information about what related offences may be committed
- to provide guidance to professionals about how to minimise risk for themselves, so that they do not inadvertently leave themselves open to allegations of professional misconduct from children and young people, or their parents / carers.

### **Definitions**

4.0 Children, young people and adults use and expertise in digital and interactive technology vary considerably. For those professionals who may have less experience of electronic technology the following definitions may be of help.

### **Digital and Interactive Technology**

4.1 The term digital (data carrying signals carrying electronic or optical pulses) and interactive (a message relates to other previous message/s and the relationship between them) technology covers a range of electronic tools. These are constantly being upgraded and their use more widespread. But it currently includes:

- the Internet which is a global system of inter-connected computers which can access the;
- World Wide Web (often shortened to the Web), which is a system of inter-linked documents accessed via the Internet. Web pages can contain text, images, and videos and other media and can be linked to other websites or pages
- mobile phones are used for voice or data communication. As well for sending and receiving voice and text communication, a mobile phone can be used for emails, accessing the Internet, gaming, Bluetooth (can send data via wireless technology), camera with video and sending and receiving photos and videos. Some new phones now have Global Positioning System (GPS) capabilities and social networking sites are including location based software.
- online gaming (using networked computers) and video game consoles (using wireless technology) and the Internet. Online games include World of Warcraft, Runescape, Final Fantasy and Lineage. Wireless video game consoles include Nintendo Wii, Microsoft Xbox and Sony Playstation

- wireless technology (a form of telecommunication using electronic magnetic waves) which enables widespread portable access to the Internet via computers, particularly laptops. It is also used for phones and radios
- broadband access which allows Internet access via computers, either desk tops or laptops. Broadband uses fibre optic cables to transmit data. Broadband penetration is now used as a key economic indicator, i.e. the number of households in a geographic area with broadband access
- webcams are video capturing devices connected to computers or computer networks. They are well-known for their low manufacturing costs and flexible applications

### **E-safety:**

4.2 This is the generic term that refers to raising awareness about how children and young people can protect themselves whilst using digital and interactive technology, and also interventions that can reduce the level of risk for children and young people using such electronic forms of communication.

### **Cyberbullying:**

4.3 Cyberbullying is bullying that takes place using digital or interactive technology. Research from the University of York shows that there is a difference in the profile of cyberbullies compared to other bullies, as noted below.

- Due to the nature of digital technology not being based on personal contact, cyberbullying breaks down the imbalance of power
- Adults working with children and young people are vulnerable to being bullied
- Adults are more likely to be targets of cyberbullies than those under 18
- It may be used as a form of revenge
- Bystanders become accessories to the bullying, e.g. through laughing at the messages and / or texts, and through distribution
- There is less understanding of its consequences, it is often the result of thoughtlessness rather than intentional
- Mobile phones are the most common tool for cyberbullies. Chat rooms are the least common
- Cyberbullying is greater outside than inside school, but its origins and consequences may be in school
- Age and gender are not significant
- Cyberbullying via chat rooms, emails, and Instant Messaging Service (IMS) has less impact on victims than other forms

### **Categories of Risk**

5.0 *Safer Children in a Digital World: The Report of the Byron Review* (DCSF, 2008) highlighted the following categories of risk to children and young people.

### **Content**

5.1 This includes illegal or inappropriate content of Internet websites, games, e-mails, mobile phones or other communication. This may include inappropriately accessing material that is of a sexual or violent nature including child abuse or adult pornography, online gaming; extremist websites which include animal rights activists, terrorism, Islamic fundamentalism or right wing extremism; websites promoting gangs and weapons; and health issues such as pro-suicide or eating disorder websites. Offences may be committed in accessing and distributing the material on such sites.

### **Conduct**

5.2 Issues related to conduct include anti-social or illegal behaviour. This includes cyberbullying that can take place via social networking sites, or other sites such as Rate my Teacher, emails, texts, and via online gaming. Cyberbullying may take the form of hate crime as an issue of race, disability and / or sexual orientation or gender identity. As stated earlier, cyberbullying can be particularly pervasive as the child or young person can receive the distressing messages or images in their own home where they should feel safe. It should be noted that those who laugh at the message / image, and / or who circulate it to others are also contributing to the cyberbullying and may be committing an offence (**see Appendix 4**).

5.3 Other issues related to conduct include children or young people being coerced, enticed or threatened into performing sexual acts via web cams. These images can then be used as a form of blackmail. Whilst some young people may think such images are solely for their 'boyfriend' for example, these can be circulated via the Internet or mobile phones to any number of others.

5.4 Any image of a child or young people could potentially be abused by posting on inappropriate websites, or by distorting through digital technology to be used in an inappropriate way. This may be of a sexual nature or of a more generic bullying nature.

### **Contact**

5.5 The risk of physical and / or sexual abuse, and resulting psychological trauma, suffered as a result of meeting someone through an online initiation is also a risk of digital technology. Adults posing as children or young people, both girls and boys, in order to groom them for the purposes of sexual exploitation, are one of the most serious concerns of the digital age. However, it is less common in comparison to cyberbullying for example. Grooming does take place via e-communication and a list of Risk Indicators is available in **Appendix 3**.

### **Commerce**

5.6 The fourth category of risk to children and young people is through commercial exploitation. This may take place through online gambling, or

financial scams, for example. Online gaming and sites such as Second Life (3-D Virtual world), encourage users to spend money through electronic transactions. Children and young people, particularly those with personal access to money, may be open to being financially exploited. Advertisers use information from IM directory of users to target SPIM (SPAM through Instant Messenger).

5.7 Currently, one of the most significant trends is that of convergence, both in terms of technology and behaviour. Types of on-line environments mentioned above, such as social networking, online gaming, instant messaging and photo sharing are merging to form larger social sites. This presents new kinds of risks to children as their information is available in one area and they will be more accessible as these environments increasingly incorporate instant messaging which facilitates one to one contact.

5.8 It should be noted that in all of the above categories, offences may be committed when accessing certain websites, and downloading the information contained within them. Further offences may be committed if such material is also distributed to others, whether harm was intended or otherwise.

### **Minimising Risk to Children and Young People**

6.0 One of the most important messages that we should ensure children and young people understand in relation to using digital technology is that they should not give out personal information, particularly their name, address or school, to anyone they do not know or trust. This particularly includes social networking and online gaming sites. If they have been asked for such information, they should always check with their parent or other trusted adult before providing such details. It is also important that they understand why they must take a parent or trusted adult with them if they meet someone face to face who they have only previously met on-line

6.1 Educating children and young people to this effect is the responsibility of all those working with them when using computers, whether that be in schools, youth clubs, residential children's homes, home education service etc. Firewalls and filtering software alone will not protect them; we need to give advice and guidance to ensure they have a safe online experience.

6.2 Supporting parents to safeguard their children:

We need to ensure that those who care for children are equipped with the knowledge and understanding of how to keep them safe and what to do if things go wrong.

6.3 Often parents do not use these environments and therefore lack confidence in supervising their children's online activities. It is important that we support parents by raising awareness of the benefits, risks and dangers to help them understand more about what their children are doing online. We need to offer practical advice and guidance on how to keep their family safe online.

6.4 Adhering to Acceptable Use Policies in all establishments:

There is a requirement to ensure that children, young people and staff use the internet and related technologies appropriately and safely. The implementation of an acceptable use policy should be built into existing policies and procedures and should provide a structure to safe e-safety practice. Acceptable use policies should clearly identify ways in which these technologies can and cannot be used and the procedures and support strategies for misuse. Please see **Appendix 1** of this policy for an exemplar Acceptable Use Policy.

## 6.5 Firewalls

While there is no guaranteed method of protecting users when on line, there are some software solutions that can filter or block content. The majority of schools obtain their Internet feed from the Regional Broadband Consortium, e.g. Yorkshire and Humber Grid for Learning, which provides a level of filtering agreed with Local Authorities and schools. There is the facility for schools to choose their own filtering requirements from within the general provision.

In other settings, where the Internet feed is not filtered, then individual machines can have specific filtering software applied. This needs to be undertaken with the agreement of senior management.

## **Procedures for Reporting Concerns**

7.0 If you are concerned that an offence has been committed, or a child or young person is at risk due to their, or another's, use of digital or interactive technology, the following steps should be taken.

**In an emergency, do not delay – ring South Yorkshire Police – dial 999.**

7.1 If you are concerned that a child or young person is suffering, or is at risk of suffering significant harm, you should make a telephone referral to Children's Social Care, in the area where the child lives:

Assessment Team West .....01226 772423  
(Central, north west, Hoyland, Penistone, Darton, Dodworth, South West, Park, Ardsley, Worsbrough)

Assessment Team East.....01226 438831  
(Brierley, Cudworth, Athersley, Royston, Monk Bretton, Dearne, Wombwell, Darfield)

7.2 This particularly relates to concerns that you think a child has been physically or sexually abused. You should follow up your telephone referral with written confirmation within **48 hours**. For further information, see Barnsley Safeguarding Children Boards' Child Protection Procedures 2007, Chapter 5: Referring Concerns to Children's Social Care or the Police.

'In general, if the concern is about abuse or risk of abuse by **someone known to the child or the child's family**, an enquiry should be made to the list/register of children who have a child protection plan. This should be followed by a referral to children's social care, if appropriate. Children's

social care should involve the police in cases where a criminal offence may have been committed.

If the concern is about abuse or risk of abuse by **someone not previously known to the child or the child's family**, a list/register check should be made and the matter should be reported directly to the police. The police **should** initiate a strategy discussion involving children's social care and other agencies, if there are wider child welfare concerns within the family.'

7.3 This section also includes guidance about talking to parents / carers (5.4). If your concern is about cyberbullying, commercial exploitation, inappropriate or illegal content of websites etc, but you do not think a child or young person is at risk of significant harm, then you should ring South Yorkshire Police (0114 220 2020) and ask to speak to the relevant Safer Neighbourhood Team, to report the incident/s.

7.4 You can obtain advice and be signposted to the relevant agency with any query relating to digital or interactive technology from **Barnsley Safeguarding Children's Unit on (01226) 772400 (Mon – Fri, 9am – 5pm)**.

## **References**

Becta: the Government agency ensuring effectiveness and innovative use of technology throughout learning <http://www.becta.org.uk/>

Code of professionalism and conduct General Teaching Council for Scotland 2008  
[http://www.gtcs.org.uk/Publications/GuidanceforTeachers/Guidance\\_for\\_Teachers.aspx?](http://www.gtcs.org.uk/Publications/GuidanceforTeachers/Guidance_for_Teachers.aspx?)

*Safer Children in a Digital World: The Report of the Byron Review* (DCSF, 2008) <http://www.dcsf.gov.uk/byonreview/>

Second Life <http://secondlife.com/whatis/>

Barnsley Safeguarding Children Boards' Child Protection Procedures 2007  
<http://www.safeguardingchildrenbarnsley.com/sqc/professionals/Policies%20and%20Procedures>

**Barnsley Safeguarding Children Board**

**E-Safety:**

**Acceptable Use Policy**

**May 2009**

<b>Title of Protocol</b>	<b>E-safety: Acceptable Use Policy</b>	
<b>Application</b>	<b>All BSCB partner agencies</b>	
<b>Date of initial ratification</b>	<b>May 2009</b>	
<b>Date of next review</b>	<b>May 2010</b>	
<b>Section</b>	<b>Contents</b>	<b>Page No.</b>
1.0	Introduction	12
2.0	Benefits of the Internet for Children and Young People	13
3.0	Managing Internet Use in Organisational Settings	14
4.0	Publishing Images and Work on the Internet	14
5.0	Managing other Technologies	17
6.0	Assessing Risk	17
7.0	Handling E-safety Complaints	18
8.0	Communicating the Contents of this Policy	18
Appendix A	E-safety Quick Self-Audit for Manager	20
Appendix B	Flow Chart for Responding to E-safety Incidents in Organisations	21
Appendix C	Guidance for Children at Key Stage 1 and 2	22
Appendix D	E-safety Rules for Young People & Acceptable Use Policy	23
Appendix E	Parental Consent Forms & Acceptable Use Policy	26
Appendix F	Teaching and Support Staff Acceptable use Policy	28

## **Introduction**

1.0 E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology - including computers, mobile phones and online games - and provides safeguards and awareness for users to enable them to control their online experiences.

1.1 All partner organisations of Barnsley Safeguarding Children Board should assess the level of risk associated with the use of digital and interactive technology by children and young people in their care. Each agency needs to take appropriate steps to safeguard children, young people and staff, according to the level of risk identified. Because of the diverse nature of the work of our partner agencies, this will vary in each organisation. This Acceptable Use Policy provides overarching guidance to all agencies in Barnsley to safeguard children and young people. It can be adapted and used accordingly within each setting. It should also operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

1.2 E-safety depends on effective practice at a number of levels:

- responsible ICT use by all staff, children and young people; encouraged by education and awareness raising and made explicit through published policies
- support and guidance for parents, giving them the knowledge and confidence to be able to supervise their child's use of digital and interactive technology
- sound implementation of e-safety policy in both administration and raising awareness, including secure network design and use
- safe and secure broadband from the Yorkshire and Humberside Grid for Learning where applicable, or other firewalls, including the effective management of content filtering
- network standards and specifications.

1.3 This policy provides guidance for agencies in relation to these issues. It specifically relates to the use of computers in organisations; it does not cover the use of mobile phones by children and young people. Organisations should have separate guidance in relation to this issue.

1.4 Each organisation should appoint an e-safety coordinator to take responsibility for this issue within the setting, and liaise with BSCB as necessary. In many cases this will be the Designated Child Protection Lead / Officer, as the roles overlap.

1.5 Acceptable Use Policies specifically agreed for primary and secondary schools in Barnsley are available via the Barnsley Safeguarding Children Board website:

<http://www.safeguardingchildrenbarnsley.com/sqc/professionals/E-Safety>

1.6 Barnsley Safeguarding Children Board acknowledges the work of Sheffield Children and Young People's Directorate, Sheffield Safeguarding Children Board, and Kent County Council in providing content in this document.

### **Benefits of the Internet for Children and Young People**

2.0 The purpose of Internet use in organisations is to raise educational standards, to promote achievement of children and young people, to support the professional work of staff and to enhance the organisation's management information and administration systems.

2.1 Internet use is an essential element in 21st century life for education, business and social interaction. It is also part of the statutory curriculum. In order to better equip children and young people for the future, the Government's Home Access Programme will soon allow broadband access in every family home in the country. Therefore our organisation has a duty to provide children and young people with quality Internet access and equip them with the skills to be safe whilst using digital and interactive technology.

2.2 Benefits of using the Internet include:

- access to world-wide educational resources including museums and art galleries
- educational and cultural exchanges between children and young people world-wide
- access to experts in many fields for children and young people and staff
- professional development for staff through access to national developments, educational materials and effective professional practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of professional issues and administration data between local, regional and national organisations
- access to learning and communication wherever and whenever convenient.

2.3 The organisation's Internet access will be designed expressly for children and young people's use and includes filtering appropriate to the age of children and young people.

2.4 Children and young people will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

2.5 Internet access will be planned to enrich and extend learning and personal development activities.

2.6 Staff will guide children and young people in on-line activities that will support learning outcomes, which are planned according to their age and maturity.

2.7 Children and young people will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### **Managing Internet Use in Organisational Settings**

3.0 This section provides guidance about how to manage the use of the Internet in the organisation. Children and young people should be provided with guidance in computer rooms, such as that in **(Appendix B, C and D)**.

### **Authorised Internet Access**

3.1 The organisation will maintain a current record of all staff and children and young people who are granted Internet access.

3.2 All staff must read and sign the 'Information Systems Code of Conduct' or similar before using the organisation's ICT resource **(see Appendix F)**.

3.3 Parents / carers will be informed that children and young people will be provided with supervised Internet access.

3.4 Parents / carers will be asked to sign and return a consent form for children and young people's access **(see Appendix E)**.

### **World Wide Web**

3.5 If staff or children and young people discover unsuitable sites, the URL (address), time, content must be reported to the designated manager or helpdesk within the organisation. via the e-safety coordinator or network manager.

3.6 The organisation will ensure that the use of Internet derived materials by children and young people and staff complies with copyright law.

3.7 Children and young people should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

### **Email**

3.8 Children and young people may only use approved e-mail accounts on the organisation system.

3.9 Children and young people must immediately tell a member of staff if they receive offensive e-mail.

3.10 Children and young people must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

3.11 Class or group e-mail addresses should be used where possible

3.12 Access to external personal e-mail accounts may be blocked.

3.13 E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on organisation headed paper.

3.14 The forwarding of chain letters is not permitted.

3.15 Children, young people and their families should only contact members of staff of organisations using business email addresses or telephone numbers. This includes staff who they knew before becoming service users of the organisation. Any exceptions to this should be discussed with managers within the organisation. This is to safeguard the children, young people, their families and the member of staff from allegations of misconduct. For further information please see **Appendix 6 of the BSCB E-safety Protocol**.

### **Social Networking**

3.16 Organisations should block/filter access to social networking sites and newsgroups unless a specific use is approved.

3.17 Children and young people and staff should be advised never to give out personal details of any kind which may identify them or their location.

3.18 Children and young people and staff should be advised not to place personal photos on any social network space.

3.19 Children and young people should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others.

3.20 Children, young people and their families should not contact members of staff via social networking sites. Staff should not accept them as friends on social networking sites and should be encouraged to review information posted about them on such sites. For further information please see **Appendix 6 of the BSCB E-safety Protocol**.

### **Filtering**

3.21 The organisation will work in partnership with the Local Authority, Becta and their Internet Service Provider to ensure filtering systems are as effective as possible.

### **Video Conferencing**

3.22 If the organisation uses video-conferencing the following issues should be considered:

- IP video-conferencing should use the relevant broadband network to ensure quality of service and security rather than the Internet.
- Children and young people should ask permission from the supervising member of staff before making or answering a video-conference call.
- Children and young people using video-conferencing will be appropriately supervised.

### **Information System Security**

3.23 The organisation's ICT systems capacity and security will be reviewed regularly, by the ICT department or agreed contractor.

3.24 Virus protection will be installed and updated regularly.

3.25 Security strategies should be discussed with the organisation's senior management team.

### **Protecting Personal Data**

3.26 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

### **Use of digital and video images - Photographic, Video**

4.0 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: (select / delete as appropriate)

4.1 • When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix)
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

### **Published Content and the Organisation Web Site**

4.2 The contact details on the organisation's web site should be the address, e-mail and telephone number. Personal information about staff, including volunteers, children, young people or their families should not be published.

4.3 Management should have overall editorial responsibility and ensure that content is accurate and appropriate.

### **Managing other Technologies**

5.0 Emerging technologies will be examined for educational and developmental benefit and a risk assessment will be carried out before use in the organisation is allowed.

5.1 Children and young people should not use mobile phones during time spent with staff from the organisation, without prior agreement from a relevant member of staff, e.g. teacher or key worker.

5.2 If children or young people send abusive or inappropriate text messages, this will be dealt with by a relevant member of staff, e.g. a teacher or key worker and may result in action being taken.

5.3 Staff will be issued with an organisation phone where contact with children and young people is required. They should not use their personal mobile phone to contact children, young people or their families. For further information please see **Appendix 6 of the BSCB E-safety Protocol**.

### **Assessing Risk**

6.0 The organisation will take all reasonable precautions to prevent access to inappropriate material. However, due to the international access available via the Internet, it is not possible to guarantee that unsuitable material will never

appear on an organisation's computer. Neither the organisation nor Barnsley Safeguarding Children Board can accept liability for the material accessed, or any consequences of Internet access.

6.1 Any child, young person or member of staff who inadvertently accesses inappropriate sites or materials should immediately report the incident to the designated e-safety lead officer and ICT department in the organisation.

6.2 The organisation should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

6.3 Computers within the organisation should not be available to anyone outside of normal working hours, e.g. if a school or youth club is used in the evenings or at weekends. The computer room should be locked in such circumstances. It should also not be available to those who do not normally require to use such equipment e.g. caretakers, maintenance personal etc.

### **Handling E-safety Complaints**

7.0 Complaints of Internet misuse will be dealt with by the line manager as per the organisation's code of conduct.

7.1 Any complaint about staff misuse must be referred to a manager. This may either be the complainant's line manager, or the manager of the member of staff about who the complaint is being made. This may invoke the Barnsley Safeguarding Children Board Allegations against Staff, Volunteers or Carers Protocol

(<http://www.safeguardingchildrenbarnsley.com/sgc/Documents/Safeguarding%20Children/Allegations%20Against%20Professionals%20procedures%20BS%20CB%20-.pdf> )

7.2 Complaints of a child protection nature must be dealt with in accordance with the organisation's internal policy and Barnsley Safeguarding Children Boards' Child Protection Procedures 2007

<http://www.safeguardingchildrenbarnsley.com/sgc/professionals/Policies%20and%20Procedures>

7.3 Children and young people and parents / carers will be informed of the complaints procedure.

7.4 Discussions will be held with South Yorkshire Police to establish procedures for handling potentially illegal issues. They can be contacted on 0114 220 2020.

### **Communicating the Contents of this Policy**

#### **Children and young people**

8.0 Rules for Internet access will be posted in all networked rooms.

8.1 Children and young people will be informed that Internet use will be monitored.

**Staff**

8.2 All staff will be given a copy of this policy, its importance explained and asked to sign the code of conduct.

8.3 Staff should be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

**Parents / carers**

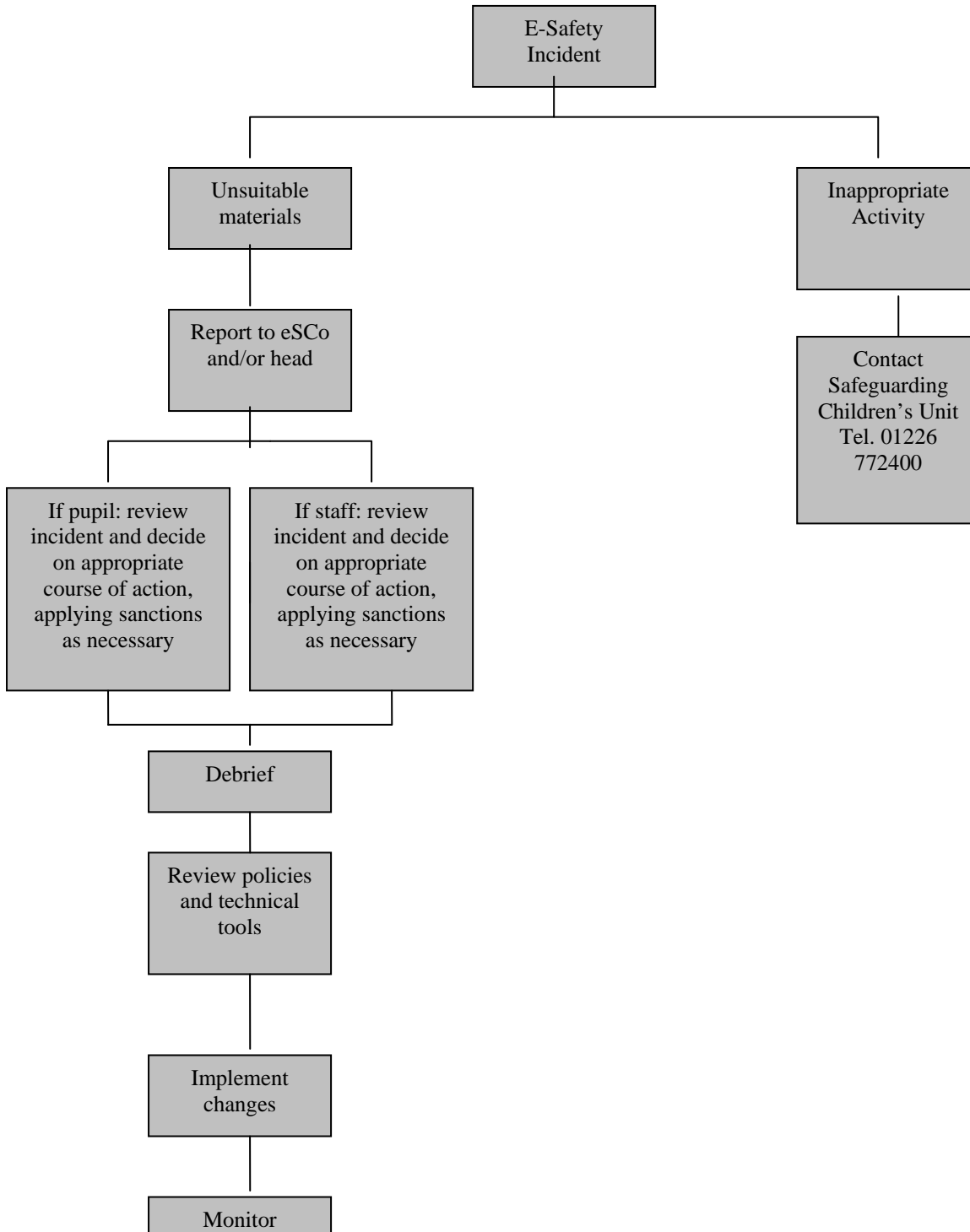
8.4 Parents / carers' attention will be drawn to this e-Safety Policy in newsletters, the organisation brochure and on the organisation's web site.

**E-Safety Quick Self-Audit for Managers**

This quick self-audit will help the senior management team in any organisation assess whether the e-safety basics are in place.

Has the organisation got an e-Safety Policy that complies with BSCB guidance?	Y/N
Date of latest update:	
The Policy was agreed by management on:	
The Policy is available for staff at:	
And for parents / carers at:	
The designated Child Protection Lead / Officer is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both children and young people and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents / carers sign and return an agreement that their child will comply with the E-safety Rules?	Y/N
Have E-safety Rules been set for children and young people?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Y/N
Has the filtering policy been approved by senior managers?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Flowchart for responding to e-safety incidents in school



## Guidance for Children at Key Stage 1 and 2

## Key Stage 1

## Think then Click

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.



We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.



B. Stoneham & J. Barrett

## Key Stage 2

## Think then Click

## E-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Adapted from Becta – E-safety 2005

### E-Safety Rules for Young People

These e-safety rules help to protect children and young people and the organisation by describing acceptable and unacceptable computer use.

- The organisation owns the computer network and can set rules for you to use it.
- It is against the rules of this organisation to use a computer or network for a purpose that we have not allowed.
- You can commit crimes by using a computer or network for a purpose we have not allowed. You may not realise you have accessed something you shouldn't until after you have done so.
- Irresponsible use may result in you being denied access to the Internet.
- If you have been given an authorised account and password for computer use, it must not be given to any other person apart from a relevant member of staff.
- All network and Internet use must be appropriate to education, personal development or communication.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, especially as they will reflect on our organisation.
- Anonymous messages and chain letters are not permitted.
- You must take care not to reveal personal information through email, personal publishing of photographs or other images, blogs or messaging.
- The organisation ICT systems may not be used for private purposes, unless you are given specific permission by a member of staff who supervises your computer use or your key worker.
- Use of the organisation's computers for personal financial gain, gambling, political activity, advertising or illegal purposes is not allowed.

This organisation may exercise our right to monitor the use of our computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where we believe unauthorised use of our systems may be taking place, or the systems may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**This poster should be displayed near computers**

# Students / pupils

## Acceptable Use Policy:

### Roles and Responsibilities

- **are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.** (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

### Policy Statements Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways: (statements will need to be adapted, depending on the age of the students / pupils and the school's structure)

- **A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
- Students / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## Student / Pupil Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil

Group / Class

Signed

Date

# Parents / Carers Acceptable use Policy:

## Roles and Responsibilities

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- **endorsing (by signature) the Student / Pupil Acceptable Use Policy**
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

(Schools should be aware of the need to consider how parental access will be covered in the e-safety policy in preparation for the introduction of online reporting to parents / carers in the coming years.)

## Policy Statements Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through: (select / delete as appropriate)

- Letters, newsletters, web site, VLE
- Parents evenings
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)

## Parent / Carer Acceptable Use Policy Agreement Template

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

# Teaching and Support Staff Acceptable Use Policy:

## Roles and Responsibilities

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**
- **they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Headteacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction**
- **digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level** and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

## Policy Statements Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select / delete as appropriate)

- **A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.** It is expected that some staff will identify e-safety as a training need within the performance management process.

• **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**

• The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.

• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

• The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

### **Staff (and Volunteer) Acceptable Use Policy Agreement Template**

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

**Assessing Risk and Identifying Problems for Children and Young People using Digital and Interactive Technology**

Universal	Vulnerable	Complex	Acute
<ul style="list-style-type: none"> <li>• Has a range of IT skills &amp; understands how digital / interactive technology works</li> <li>• Safely enjoys the benefits of digital / interactive technology &amp; is able to communicate safely with friends &amp; family</li> <li>• Maintains personal security when using digital / interactive technology</li> <li>• Family aware of use &amp; understand safe use principles</li> <li>• Child shares interest with parents</li> </ul>	<ul style="list-style-type: none"> <li>• Some IT skills but not really understanding of how digital / interactive technology works</li> <li>• Uses digital / interactive technology carelessly, visiting unregulated sites &amp; communicating with unknown others</li> <li>• Visits adult sites &amp; views explicitly sexual or violent material</li> </ul>	<ul style="list-style-type: none"> <li>• Has IT skills, but using them to access unsuitable areas of digital / interactive technology. Or has poor IT skills &amp; is vulnerable because of this</li> <li>• Uses digital / interactive technology to establish contact with unknown others &amp; discloses personal contact details</li> <li>• Visits illegal sites or sites designed for adults &amp; develops an interest which may lead to criminal or exploitative actions</li> <li>• Exposes friends to risk by disclosing details to strangers</li> </ul>	<ul style="list-style-type: none"> <li>• Has IT skills &amp; accesses unsuitable sites or has poor IT skills &amp; is therefore vulnerable to exploitation by others</li> <li>• Transmits picture of self which could be used by digital / interactive predator</li> <li>• Posts explicitly sexual material including photos of self</li> <li>• Discloses address &amp; phone details</li> <li>• Agrees to meet stranger</li> <li>• Discloses stranger abuse resulting from Internet contact</li> </ul>

**Indicators of Risk of Sexual Exploitation via Digital and / or Interactive Technology**

**At Risk**

- Spending increasing amount of time on social networking sites ( e.g. Bebo, MSN, My Space, Facebook)
- Accessing dating agencies via mobile phone ( e.g. 02 flirt line)
- Unexplained increased mobile phone /gaming credits
- New contacts with people out of city
- Spending increasing amounts of time with on line friends and less time with friends from school or neighbourhood
- Going on line during the night
- Being secretive. Using mobile phone for accessing Bebo etc more than computers
- Unwilling to share /show on line contacts
- Concern that a young person's online friendship has developed into an off line relationship
- Concern that inappropriate images of a young person are being circulated via the internet

**Swapping**

- Arranging to meet people they have met on line
- Exchanging inappropriate images in exchange for gaming knowledge/phone and gaming credits
- Receiving gifts through the post from someone the young person does not know
- Concern that a young person is having an online relationship
- Concern that a young person is being coerced to provide images
- Sharing of inappropriate images amongst friends

**Selling**

- Concerned that a young person is being bribed by someone for their inappropriate on line activity
- Concern that a young person is selling images via the internet for money
- Concern that a young person is being drawn into providing increasingly provocative/sexualised images in exchange for payment
- Negotiating a price for sexual activity/images
- Concern that a young person is selling sexual services via the internet

**South Yorkshire Police - Cyber Bullying & Crime Potential Offences**

This is not an exhaustive list

<b>OFFENCE</b>	<b>Home Office Description</b>	<b>Home Office Group</b>
Abuse of position of trust: causing or inciting a female child to engage in sexual activity (offender is aged 18 or over & victim is 13 - 17)	<i>Abuse of position of trust of a sexual nature</i>	SEXUAL OFFENCES
Abuse of position of trust: causing or inciting a male child to engage in sexual activity (offender is aged 18 or over & victim is under 13)	<i>Abuse of position of trust of a sexual nature</i>	SEXUAL OFFENCES
Aid/abet suicide	<i>Aiding suicide</i>	OTHER NOTIFIABLE OFFENCES
Arranging or facilitating the commission of a child sex offence	<i>Abuse of children through prostitution &amp; pornography</i>	SEXUAL OFFENCES
Blackmail	<i>Blackmail</i>	OTHER NOTIFIABLE OFFENCES
Breach of anti social behaviour order & interim ASBO (order made to protect from harassment alarm or distress) (C&D act 1998 s. 1(10))	<i>Other offence against the state or public order</i>	OTHER NOTIFIABLE OFFENCES
Breach of non molestation order	<i>Other offence against the state or public order</i>	OTHER NOTIFIABLE OFFENCES
Breach of sex offender order to be used with breach of sex offender order (SOPO) & interim sex offender order (Interim SOPO)	<i>Other offence against the state or public order</i>	OTHER NOTIFIABLE OFFENCES
Causing a child to watch a sexual act (offender is aged 18 or over & victim is under 13)	<i>Abuse of position of trust of a sexual nature</i>	SEXUAL OFFENCES
Causing a child under 13 to watch a sexual act	<i>Sexual activity involving a child under 13</i>	SEXUAL OFFENCES
Causing a child under 16 to watch a sexual act	<i>Sexual activity involving a child under 16</i>	SEXUAL OFFENCES
Causing or inciting a female child under 13 to engage in sexual activity - no penetration	<i>Sexual activity involving a child under 13</i>	SEXUAL OFFENCES
Causing or inciting a female child under 16 to engage in sexual activity - penetration	<i>Sexual activity involving a child under 16</i>	SEXUAL OFFENCES
Causing or inciting a male child under 13 to engage in sexual activity - no penetration	<i>Sexual activity involving a child under 13</i>	SEXUAL OFFENCES
Causing or inciting a male child under 13 to engage in sexual activity - penetration	<i>Sexual activity involving a child under 13</i>	SEXUAL OFFENCES

Causing or inciting a male child under 16 to engage in sexual activity - no penetration	<i>Sexual activity involving a child under 16</i>	SEXUAL OFFENCES
Causing or inciting female child under 16 to engage in sexual activity - no penetration	<i>Sexual activity involving a child under 16</i>	SEXUAL OFFENCES
Committing an offence with intent to commit a sexual offence	<i>Other miscellaneous sexual offences</i>	SEXUAL OFFENCES
Communications act 2003 (triable either way offences except sections 125, 126)	<i>Other notifiable offence</i>	OTHER NOTIFIABLE OFFENCES
Conspiracy to commit fraud/deception by cheque or credit card	<i>Cheque &amp; plastic card fraud</i>	FRAUD & FORGERY
Conspiracy to defraud (apart from cheque & credit card fraud)	<i>Fraud by false representation &amp; other frauds</i>	FRAUD & FORGERY
Dishonestly obtain electronic communications services	<i>Other notifiable offence</i>	OTHER NOTIFIABLE OFFENCES
Exposure	<i>Exposure &amp; voyeurism</i>	SEXUAL OFFENCES
Fraud by false representation & other frauds - dishonestly make false representation to make gain for self/another or cause loss to other/expose other to risk	<i>Fraud by false representation &amp; other frauds</i>	FRAUD & FORGERY
Harassment - (PFHA section (3)) breach of conditions of injunction against harassment	<i>Harassment</i>	VIOLENCE AGAINST THE PERSON
Harassment - (PFHA section (4)) putting people in fear of violence	<i>Harassment</i>	VIOLENCE AGAINST THE PERSON
Harassment - (PFHA section (5)) breach of a restraining order	<i>Harassment</i>	VIOLENCE AGAINST THE PERSON
Harassment - (protection from harassment act 1997 section 2)	<i>Harassment</i>	VIOLENCE AGAINST THE PERSON
Indecent matter publicly displayed	<i>Obscene publications etc.</i>	OTHER NOTIFIABLE OFFENCES
Meeting a female child following sexual grooming etc. (offender aged 18 or over & victim under 16)	<i>Sexual grooming</i>	SEXUAL OFFENCES
Meeting a male child following sexual grooming etc. (offender is 18 or over & victim is under 16)	<i>Sexual grooming</i>	SEXUAL OFFENCES
Obtain money transfer by cheque or credit card fraud	<i>Cheque &amp; plastic card fraud</i>	FRAUD & FORGERY
Obtain pecuniary advantage by cheque or credit card fraud	<i>Cheque &amp; plastic card fraud</i>	FRAUD & FORGERY
Obtain property by deception cheque or credit card fraud	<i>Cheque &amp; plastic card fraud</i>	FRAUD & FORGERY

Obtain services by cheque or credit card fraud	<i>Cheque &amp; plastic card fraud</i>	FRAUD & FORGERY
Possessing obscene material for gain	<i>Obscene publications etc.</i>	OTHER NOTIFIABLE OFFENCES
Possession of an indecent or pseudo photograph of a child	<i>Obscene publications etc.</i>	OTHER NOTIFIABLE OFFENCES
Possession of racially inflammatory material	<i>Other offence against the state or public order</i>	OTHER NOTIFIABLE OFFENCES
Public order - cause intentional harassment, alarm or distress (POA 1986 s. 4a)	<i>Public fear alarm or distress (POA 1986 secs 4,4a&amp;5)</i>	VIOLENCE AGAINST THE PERSON
Public order - fear or provocation of violence (POA 1986 s. 4)	<i>Public fear alarm or distress (POA 1986 secs 4,4a&amp;5)</i>	VIOLENCE AGAINST THE PERSON
Public order - harassment alarm or distress (POA 1986 s. 5)	<i>Public fear alarm or distress (POA 1986 secs 4,4a&amp;5)</i>	VIOLENCE AGAINST THE PERSON
Racial hatred - publishing or distributing written material intended or likely to stir up racial hatred	<i>Other offence against the state or public order</i>	OTHER NOTIFIABLE OFFENCES
Racial hatred - use of words or behaviour or display of written material intended or likely to stir up racial hatred	<i>Other offence against the state or public order</i>	OTHER NOTIFIABLE OFFENCES
Racially aggravated fear or provocation of violence section 31(1)(a)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Racially aggravated harassment (C&D act 1998 s. 32(1)(a),(3))	<i>Racially or religiously aggravated harassment (excludes offences under 9b)</i>	VIOLENCE AGAINST THE PERSON
Racially aggravated harassment, alarm or distress section 31(1)(b)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Racially aggravated intentional harassment, alarm or distress section 31(1)(b)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Racially aggravated put people in fear of violence s. 32(1)(b),(4)	<i>Racially or religiously aggravated harassment (excludes offences under 9b)</i>	VIOLENCE AGAINST THE PERSON
Racially or religiously aggravated harassment, alarm or distress section 31(1)(b)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON

Racially or religiously aggravated intentional harassment, alarm or distress section 31(1)(b)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Racially or religiously aggravated offence of harassment s32 (1) (a), (3)	<i>Racially or religiously aggravated harassment (excludes offences under 9b)</i>	VIOLENCE AGAINST THE PERSON
Religiously aggravated fear or provocation of violence section 31(1)(a)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Religiously aggravated harassment, alarm or distress section 31(1)(b)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Religiously aggravated intentional harassment, alarm or distress section 31(1)(b)	<i>Racially or religiously aggravated public fear alarm or distress</i>	VIOLENCE AGAINST THE PERSON
Telecommunications act 1984 secs 5,28,29,42(1),44,45,46,53(2)(3)(4),101.	<i>Other notifiable offence</i>	OTHER NOTIFIABLE OFFENCES
Using data for unauthorised purpose; disclosing data to unauthorised person etc (triable either way offences)	<i>Other notifiable offence</i>	OTHER NOTIFIABLE OFFENCES
Voyeurism	<i>Exposure &amp; voyeurism</i>	SEXUAL OFFENCES

### **How to Work Safely with Information and Communication Technology** **(adapted from Becta guidance)**

ICT offers a range of benefits for teaching, learning and social networking, but all computers and devices need to be used with care. This material looks at the health and safety issues involved in using computers in general, in classrooms and other venues where children use computers.

Computers and peripherals such as printers are electrical equipment, so there are some general points to consider:

- Ensure that all electrical installations are carried out by a qualified electrician.
- All equipment must be of a reliable standard and should be checked annually by qualified electricians.
- Ensure that no cabling is trailing on the floor.
- Ensure that seating is suitable for the size of children using it.
- Ensure that benching is sturdy enough to withstand the weight of the hardware and additional equipment stored on it.
- Follow health and safety guidance regarding the height, position and distance of monitors and keyboards from children when working.
- If you are using a data projector, make sure that all leads are safely located, and that children don't walk around the back of working areas which have cables.
- If you are using an interactive whiteboard, ensure that all children can reach it without standing on anything.
- If using data projectors or interactive whiteboards, ensure that children never look directly into the beam of the projector. If presenting to a class or other setting and entering the beam, children should not look towards the audience for more than a few seconds, and ideally should keep their backs to the beam at all times.
- Children should be supervised at all times during the operation of data projectors or interactive whiteboards. Ensure that they never look directly into the beam of the projector, and if presenting to a class or other setting entering the beam, children should not look towards the audience for more than a few seconds. Ideally they should keep their backs to the beam at all times.
- If you are working with programmable toys such as floor turtles, create a clearly defined working area; use markers or seating to define the work space to ensure that children do not accidentally fall over equipment.

#### **Working safely in the ICT suite**

Children should be aware of rules for using computers. Ideally, they will be involved in devising these rules and may make posters explaining why the rules are necessary.

- Fire exits must be kept clear at all times; do not allow them to be blocked by equipment or pupils' bags.
- If children are going to be seated for extended periods, ensure that good-quality seating is provided which supports the back.
- Seating should be height-adjustable so that monitors and keyboards are correctly positioned and children do not have to look up or down at the monitor for prolonged periods.
- Check to see if there is too much reflected light on monitor screens, making it difficult for children to see.
- Ensure that children can see displays adequately.
- Make sure that children have room to make notes or use textbooks alongside the computer.
- Ensure that the room temperature does not get too warm because computers are kept switched on for prolonged periods.
- Ensure that there is enough fresh air circulating; installing a fan simply moves the warm, stale air about without renewing it.

### **Working safely in classrooms and other settings**

There are some issues that are more relevant to working on computers in classrooms and other settings:

- Locate the computers in areas where children can sit and work without distracting or disrupting others in the class.
- Ensure that procedures for connecting peripherals (scanners, digital cameras, webcams, control technology equipment and monitoring equipment), adhere to school and local authority health and safety guidelines.
- Ensure that additional equipment is situated where it will not cause a hazard such as trailing cables.
- If you are using laptops, ensure that they are located on firm desks or tables.
- Ensure that all electrical equipment is located away from water supplies, and that children have a sound knowledge of electrical safety.
- Ensure that children don't take drinks to tables if they are working with electrical equipment such as cameras, videos, laptops, computers or data logging equipment.

If you have a number of portable computers in the classroom or other setting, you may want to set up a procedure to be followed when they are to be moved. For example, you could stipulate that only a small group of children should move at a time, or designate specific children to be responsible for laptops.

[http://schools.becta.org.uk/index.php?section=lv&catcode=ss\\_lv\\_saf\\_hs\\_03&id=2348](http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_hs_03&id=2348)

### **Minimising Risk of Allegations of Professional Misconduct**

#### **Guidance for all Professionals working with Children and Young People or their Families, in Barnsley**

All agencies will have their own professional codes of conduct, which this guidance does not intend to replace. It is guidance that relates specifically to helping professionals put safeguards in place to minimise the risk of any allegations of professional misconduct related to the use of digital or interactive technology.

This guidance relates to all children up to the age of 18, whether or not they, or their families, are current or former service users. It is appreciated that you may have personal friends or the children of friends who are under the age of 18. But at all times you should ensure that you treat all those under the age of 18 with the respect they deserve, whoever the child or young person is.

You should always be mindful not to put yourself in a situation that may comprise you or be misinterpreted either by the child or young person, their friend, parent or carer, or any other person. This includes both personal and professional situations. It should be remembered that careless and inappropriate action in a personal setting, whether intended or not, could have significant implications for your professional life.

There are few professionals who have allegations of professional misconduct related to digital and interactive technology made against them, or who are the victims of cyberbullying from children, young people, their friends or families. However, the impact of either an allegation or cyberbullying can be significant, both personally and professionally. Taking a few steps to be proactive in minimising any risk to yourself, whilst you may think it unnecessary, is worth taking to avoid future complications.

Remember: as a professional working with children and young people, or their families, you may be vulnerable to have an allegation made against you or being the victim of cyberbullying. Sometimes this is a result of communication or a situation being misconstrued. Other times this may be an act of revenge taken against you for an incident that has resulted through your professional practice. It may also be that someone, through having complex needs of their own, may develop an unhealthy interest in you as a person.

Therefore the following steps are recommended to all professionals, and trainees who are or will be working with children, young people or their families.

## Ten Steps to Minimise Professional Risk

- 1) As a professional you should fully appreciate that the onus is upon you and not the child or young person to distance yourself from any potentially inappropriate situation.
- 2) Review all content about yourself on social networking sites, such as Face Book, My Space etc. Particularly consider removing any personal information or photographs. These could be manipulated and used against you.
- 3) Do not give personal information such as email addresses or mobile telephone numbers to anyone who is, or has been, a service user or is a member of their family.
- 4) If you wish to keep in contact with any child or young person under the age of 18, or their family, who has been a user of your service, ensure that you only use work emails or telephone numbers to communicate with them.
- 5) If there is any incident, related to this guidance, which involves a child, young person or their family, that causes you concern, report it immediately to your line manager. Document it as soon as possible, according to your workplace procedures.
- 6) Ensure you adhere rigidly to the Acceptable Use Policy of your workplace. If you breach any part of the AUP, report it immediately as per your workplace procedures.
- 7) Do not access any illegal or inappropriate websites on your personal computer or mobile phone. This includes illegal or inappropriate images of children, certain other types of pornography or extremist websites. It is illegal to access or download material that promotes or depicts criminal behaviour.
- 8) Be very careful when liaising with others in contact / web cam internet sites (for example chat rooms, message boards, social networking sites and newsgroups). Avoid inappropriate communication with individuals under 18, or with who you may be in a position of trust. Avoid inappropriate communication with those who you do not know. Adults can pose as children using interactive technology; likewise some children can pose as adults.
- 9) Use your common sense and professional judgement and expertise at all times to avoid circumstances which are, or could be, perceived to be of an inappropriate nature. This relates particularly to social networking sites and mobile phone technology.
- 10) Remember, digital and interactive technology may be the virtual world, but it has an impact on our real world. Do not treat people any differently through electronic communication than you would on a personal basis.

Below are examples from the media of digital and interactive technology issues for professionals.

Sheffield Star, 11 November 2008

### **Sex website anguish**

A LEADING Sheffield businessman and parish councillor made the shocking discovery that his photo and personal details had been plastered on sex websites.

Married father-of-one Simon Bower was horrified to find he had been appearing on gay dating services - after a tip off from a friend. Profiles including his photo, age, height and weight had been posted on three websites. There was even a poll asking browsers to rate his looks.

Mr Bower, managing director of Pollards coffee shop and Ecclesfield parish councillor, called in solicitors to get the details removed.

The 39-year-old had used the social networking site Facebook but now wants to warn other people about the dangers of the internet.

He said: "I had a phone call from a friend to say he had seen my photo on a sex website. Somebody had set me up and was purporting to be me.

"When I began to search around, I found other sex websites with my profile on them. The photos had been taken off my Facebook page and also from a business networking site.

"It also had my age, height and they had guessed my weight. My wife and I can just about laugh at it now but it was very embarrassing and shocking. I'm not gay, I'm married with a two-year-old daughter and it was very fortunate that my wife was understanding."

Mr Bower's solicitors contacted the websites and demanded the information be removed. He added: "It's possible I did put myself at risk by being on Facebook but I couldn't believe how easy it was to steal photos from websites, with just a click of a mouse.

"It's breathtaking and very annoying that you can do this anonymously without being traced."

Mr Bower's solicitor Hazel Randall said the case did not amount to identity theft because the details were used to cause embarrassment rather than commit fraud. But she warned that such incidents were becoming more common - and that it was difficult to track down the culprit.

Hazel, an associate at DLA Piper who specialises in law surrounding technology, said: "If someone stole Mr Bower's details to open a fake bank account then that would be a criminal matter but if it's just to embarrass him it's a civil matter.

"In the first instance, you should contact the website and ask them to remove the information."

"They are obliged under European law to do this promptly or they could face libel action."

"The problem is, the information could have been on the website for months without you knowing about it."

"Most of these websites don't require proper contact details so there's no way of finding out who did it."

**Cyber bullying threat to teachers****Teachers are calling for much tougher restrictions to protect staff from "cyber bullying" by pupils.**

The Association of Teachers and Lecturers has warned of the distress caused to teachers by anonymous, malicious comments on websites.

"Offensive" comments and mocking video clips should not be allowed to undermine teachers' authority.

Such public attacks "belittle and bully" classroom teachers, says the teachers' union.

The union's general secretary Mary Bousted says that the public mockery of teachers "robs them of dignity and self-esteem".

Such "verbal abuse" needed to be curbed, the union says - and it is calling on the government to "take all reasonable steps to protect the integrity" of teachers.

**Legal powers**

In response, a spokesperson for the Department for Education and Skills says that: "Teachers now have stronger legal powers to deal with cyber pests as part of our continued fight against bullying.

"They can now confiscate mobile phones which are being used in a malicious or disruptive way. We encourage them to make full use of this power."

A survey quoted by the union claimed that 45% of teachers had received an attack by e-mail, 15% had received threatening texts - and that 10% had been upset by messages written about them on websites. Andy Brown, a teacher at Ballymena Academy in Northern Ireland, told the union's annual conference in Bournemouth that staff were being harassed by anonymous insults on websites.

These included doctored images designed to ridicule teachers - and allegations or innuendo about their professional ability and personal lives.

Mr Brown described a secondary teacher who had been pushed into early retirement by a "campaign of derogatory and false statements placed on a website".

"What about teachers who've had pictures taken and posted of them when they're socialising or have had comments questioning their fidelity to their partner?" he told the conference.

Mr Brown said that he had checked comments made about himself on the RateMyTeachers website - which allows pupils to publish their opinions about their teachers.

He told the conference that he had found "two negative, hurtful comments about my teaching ability and me as a person".

And even though there were many more positive and complimentary comments - the two negative comments, made anonymously and available publicly, continued to rankle.

"I've had teachers on the phone to me in tears because of comments made about them. It would be easy to say 'don't read them', but it's difficult when we invest so much of our selves not to want to know what is being said about us," said Mr Brown.

<http://news.bbc.co.uk/go/pr/fr/-/1/hi/education/6522501.stm>  
Published: 2007/04/03 16:39:00 GMT