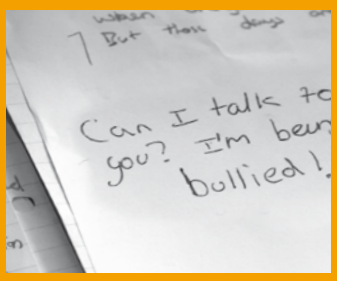
Cyberbullying



Safe to Learn: Embedding anti-bullying work in schools

department for
children, schools and families

This guidance was developed for the Department for Children, Schools and Families (DCSF) by Childnet International and in consultation with the DCSF Cyberbullying Taskforce, on which representatives of the following organisations sit (*in alphabetical order*):

Anti-Bullying Alliance (ABA)
AOL (UK) limited
Association of School and College Leaders (ASCL)
Association of Teachers and Lecturers (ATL)
BBC
Beatbullying
Bebo
Becta
Child Exploitation and Online Protection Centre (CEOP)
Childnet International
Children's Charities' Coalition for Internet Safety
Cyberspace Research Unit, University of Central Lancashire
Department for Business, Enterprise and Regulatory Reform (BERR)
Fox Interative Media / MySpace
Get Connected
Google / YouTube
Home Office
Kidscape
London Councils
Microsoft (MSN and Windows Live services)
Ministry of Justice (MoJ)
Mobile Broadband Group
National Association of Head Teachers (NAHT)
The National Association of Schoolmasters / Union of Women Teachers (NASUWT)
National Governors' Association (NGA)
National Society for the Prevention of Cruelty to Children (NSPCC)
National Union of Teachers (NUT)
O2
Orange
Parent Governors Representatives Network
Professional Association of Teachers (PAT)
The Carphone Warehouse
The Samaritans
T-Mobile UK
Unison
Unit for School and Family Studies, Goldsmiths, University of London
Vodafone
Yahoo! UK & Ireland
Youth Justice Board (YJB)
York St John University

The Department would also like to thank the staff and pupils at Avenue Primary School, Leicester, and Hamilton Community College, Leicester, for contributing to the development of this guidance.

Contents

GUIDANCE

Executive summary 03

1. Understanding cyberbullying 06
   - What is cyberbullying and why do schools need to take it seriously? 06
   - The context: young people and technology 10
   - Forms that cyberbullying can take 11
   - How is cyberbullying different to other forms of bullying? 13
   - Brief introduction to the technology 15

2. Preventing cyberbullying
   - Taking a whole-school community approach 22
   - Understanding and talking about cyberbullying 23
   - Updating existing policies and practices 24
   - Making reporting cyberbullying easier 25
   - Promoting the positive use of technology 27
   - Evaluating the impact of prevention activities 28

3. Responding to cyberbullying 30
   - Cyberbullying is a form of bullying 30
   - Support for the person being bullied 31
   - Investigation 35
   - Working with the bully and applying sanctions 37

FURTHER RESOURCES

A. Key advice to parents and carers on cyberbullying 40

B. Key advice to children and young people on cyberbullying 42

C. What children and young people say 44

D. Useful websites and resources 46

E. Case study: Letter inviting parents to cyberbullying information event 48

F. Case study: Information letter on sanctions 50

G. Case study: Example Acceptable Use Policy (AUP) 51

CYBERBULLYING: Guidance

As more and more schools are having to respond to the growing challenge of cyberbullying, it is vital that schools **understand** the issue, know how to **prevent** and **respond** to incidents, and are updated on the legal issues surrounding this challenging subject.

The DCSF has worked with children's charity **Childnet International** to provide this guidance, which forms part of the anti-bullying guidance *Safe to Learn: Embedding Anti-Bullying Work in Schools*. You will be able to find important information and clear advice on the subject, and review how your school takes action.

"The internet and mobile phones have such positive power to transform children's lives for the better. However, when they are misused, they can cause real pain and distress. Childnet is delighted to have worked with the DCSF and with members of the Cyberbullying Taskforce in drawing up this guidance which we hope will be of real practical help to schools."
Childnet International

Childnet has produced a summary of this guidance and a film for schools to use in addressing this issue, which are available at www.digizen.org

Quote from a pupil:

"I felt that no-one understood what I was going through. I didn't know who was sending me these messages, and I felt powerless to know what to do."

Quote from a parent:

"Having my daughter show me text messages from nearly everyone in her class all saying derogatory things about her was devastating."

Quote from a staff member:

"The accusation about me which the students put on their website was horrendous. Within hours it seemed that the whole school had read this message."

Executive summary

Understanding cyberbullying

1. Cyberbullying can be defined as the use of *Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.* It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

2. Research into the extent of cyberbullying indicates that it is a feature of many young people's lives. It also affects members of school staff and other adults; there are examples of staff being ridiculed, threatened and otherwise abused online by pupils.

3. Cyberbullying, like all bullying, should be taken very seriously. It is never acceptable, and a range of Education Acts and government guidance outline schools' duties and powers in relation to bullying. The Education and Inspections Act 2006 (EIA 2006) includes legal powers that relate more directly to cyberbullying; it outlines the power of head teachers to regulate the conduct of pupils when they are off-site and provides a defence in relation to the confiscation of mobile phones and other items.

4. Although cyberbullying is not a specific criminal offence, there are criminal laws that can apply in terms of harassment and threatening and menacing communications. Schools should contact the police if they feel that the law has been broken.

5. Cyberbullying takes different forms: threats and intimidation; harassment or "cyber-stalking" (e.g. repeatedly sending unwanted texts or instant messages); vilification / defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images); and manipulation.

6. Some cyberbullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyberbullying are known to be unintentional and the result of simply not thinking about the consequences. What may be sent as a joke, may not be received as one, and indeed the distance that technology allows in communication means the sender may not see the impact of the message on the receiver. There is also less opportunity for either

party to resolve any misunderstanding or to feel empathy. It is important that pupils are made aware of the effects of their actions.

7. In cyberbullying, bystanders can easily become perpetrators – by passing on or showing to others images designed to humiliate, for example, or by taking part in online polls or discussion groups. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the person targeted. It is recommended that anti-bullying policies refer to those 'bystanders' – better termed 'accessories' in this context – who actively support cyberbullying and set out sanctions for this behaviour. It is important that pupils are aware that their actions have severe and distressing consequences and that participating in such activity will not be tolerated.

Preventing cyberbullying

8. It is important to decide on the roles and responsibilities for cyberbullying prevention work. This will typically involve a named lead from the senior management team (usually the person with overall responsibility for anti-bullying work), as well as IT staff, pastoral care staff, and school council members.

9. Essential elements of prevention are awareness-raising and promoting understanding about cyberbullying. Awareness can be raised and understanding promoted through discussion and activity around what cyberbullying is and how it differs from other forms of bullying. The activities could include staff development activities; home-school events such as special assemblies with parents; and addressing cyberbullying within curriculum delivery and the Social and Emotional Aspects of Learning (SEAL) programme.

10. It is important to review and update existing anti-bullying, behaviour and pastoral care policies to include cyberbullying. Ensure that learners, parents and staff are all aware of the procedures and sanctions for dealing with cyberbullying, including bullying that takes place out of school.

11. It is advised that schools establish, or review existing, Acceptable Use Policies (AUPs), referencing responsible use of school IT networks and equipment, Virtual Learning Environments (VLEs) and mobile phones. It is also recommended that schools review how the school network is monitored and check whether existing procedures are adequate.

12. It is recommended that schools record and monitor incidents of cyberbullying in the same way as all other forms of bullying. Schools can use this information to develop their policies and practices.

13. Publicising reporting routes is an important element of prevention, raising awareness of the issue but also ensuring that any incidents can be stopped before they become too serious or upsetting. Make sure that learners, parents and staff are all aware of the different ways available to report cyberbullying incidents. In addition, schools can signpost information about external reporting routes, providing information about contacting service providers directly.

14. Education and discussion around the responsible use of technologies and e-safety are key to preventing cyberbullying and helping children and young people deal confidently with any problems that might arise, whether in or out of school. Technology can have a positive role in learning and teaching practice, and there is a need for staff to be confident about ICT in order to model the responsible and positive use of technologies and to respond to incidents of cyberbullying appropriately.

15. Stay up to date – prevention and responding strategies require continuous review and refinement as new technologies and services become popular. This guidance, similarly, will be updated periodically as technologies develop.

16. It is useful to publicise progress and cyberbullying prevention activities to the whole-school community. Keep cyberbullying a live issue and celebrate your successes.

Responding to cyberbullying

17. Cyberbullying is a form of bullying, and as such schools should already be equipped to deal with the majority of cyberbullying cases through their existing anti-bullying and behaviour policies and procedures. However, schools should recognise the ways in which cyberbullying differs from other forms of bullying and reflect that in how they respond to it. In addition to considerations about the invasiveness of cyberbullying, the size of the audience, and other such factors, cyberbullying yields evidence in a way that other forms of bullying do not.

18. The person being bullied will usually have examples of texts or emails received, and should be encouraged to keep these to aid in any investigation. There are also additional reporting routes available, through mobile phone companies, internet service providers and social networking sites. Detailed information on retaining evidence, containing incidents, and contacting the relevant organisations is provided in this guidance.

19. Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. There are advantages in trying to contain the spread of these, and options here include contacting the service provider, confiscating phones, and contacting the police (in relation to illegal content).

20. Advise those experiencing cyberbullying on steps they can take to avoid recurrence – for example, advise those targeted not to retaliate or reply; provide advice on 'blocking' or removing people from 'buddy lists'; and ask them to think carefully about what private information they may have in the public domain.

21. Take steps to identify the person responsible for the bullying. Steps can include looking at the school system and computer logs; identifying and interviewing possible witnesses; and, with police involvement, obtaining user information from the service provider.

22. Once the person responsible for the cyberbullying has been identified, it is important that, as in other cases of bullying, sanctions are applied. Steps should be taken to change the attitude and behaviour of the bully, as well as ensuring access to any help that they may need. Schools will have existing sanctions in place for bullying behaviour, and these should apply equally to cyberbullying. In addition, it is important to refer to any Acceptable Use Policies (AUPs) for internet and mobile use, and apply sanctions where applicable and practical. Technology-specific sanctions for pupils engaged in cyberbullying behaviour could include limiting internet access for a period of time or removing the right to use a mobile phone on the school site, for example.

1. Understanding cyberbullying

1.1 WHAT IS CYBERBULLYING AND WHY DO SCHOOLS NEED TO TAKE IT SERIOUSLY?

A definition

1.1.1 Cyberbullying can be defined as *the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else*. As with a school's general definition of bullying, however, it is advised that schools involve the whole school community in agreeing an accessible and meaningful definition. In this way, the school will secure greater awareness of the phenomenon and buy-in for its overall policy and strategies to tackle cyberbullying.

1.1.2 Cyberbullying is a sub-set or 'method' of bullying. It can be used to carry out all the different 'types' of bullying (such as racist bullying, homophobic bullying, or bullying related to special educational needs and disabilities), but instead of the perpetrator carrying out the bullying in person, they use technology as a means of conducting the bullying. Cyberbullying can include a wide range of unacceptable behaviours, including harassment, threats and insults. And like face-to-face bullying, cyberbullying is designed to cause distress and harm.

1.1.3 Cyberbullying can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, cyberbullying does differ in several significant ways to other kinds of bullying: for example, the invasion of home/personal space; the difficulty in controlling electronically circulated messages; and even in the profile of the bully and target. These differences are important ones for people working with children and young people to understand (see section 1.4).

1.1.4 Cyberbullying takes place between children; between adults; but also across different age groups. Young people can target staff members or other adults through cyberbullying: there are examples of school staff being ridiculed, threatened and otherwise abused online.

Quote from a head teacher:

"One of my staff members was recently the victim of cyberbullying – some of the students created a web site about them which contained nasty comments and accusations…As a direct result the member of staff suffered from depression and stress, and was actively planning to leave the school. I can honestly say that this episode nearly destroyed this man".

How common is cyberbullying?

1.1.5 There have been some studies looking at the extent of cyberbullying amongst children and young people:

- Research carried out for the Anti-Bullying Alliance (ABA) by Goldsmiths, for example, found that 22% of 11-16 year-olds had been a victim of cyberbullying[1].

- The MSN cyberbullying report (2006) found that 11% of UK teens had experienced cyberbullying[2] .

- Noret and River's four year study on bullying (2007) found that 15% of the 11,227 children surveyed had received nasty or aggressive texts and emails, and demonstrated a year on year increase in the number of children who are being bullied using new technology.

- Research conducted as part of the DCSF cyberbullying information campaign found that 34% of 12-15 year olds reported having been cyberbullied.

- Qualitative evidence gathered by NASUWT through a survey of teachers has demonstrated that cyberbullying affects the working lives of staff and impacts severely on staff motivation, job satisfaction and teaching practice.

1.1.6 Although there is variation in the figures, **all the research indicates that cyberbullying is a feature of many young people's lives**. There is also concern that the level of cyberbullying is increasing.

Legal duties and powers: Education law

1.1.7 Bullying (and this includes cyberbullying) is never acceptable. The school community has a duty to protect all its members and provide a safe, healthy environment. These obligations are highlighted in a range of Education Acts and government initiatives (see section 2 of the overarching *Safe to Learn: Embedding Anti-Bullying Work in Schools* guidance).

1.1.8 In addition, the **Education and Inspections Act 2006** (EIA 2006) outlines some legal powers which relate more directly to cyberbullying. Head teachers have the power "to such extent as is reasonable" to regulate the conduct of pupils when they are off-site or not under the control or charge of a member of staff. This is of particular significance to cyberbullying, which is often likely to take place out of school but which can impact very strongly on the school life of those pupils involved. Section 3.4 of the *School Discipline and Pupil Behaviour Polices* guidance provides more advice on when schools might regulate off-site behaviour[3] .

1.1.9 EIA 2006 also provides a defence for school staff in confiscating items from pupils. This can include mobile phones when they are being used to cause a disturbance in class or otherwise contravene the school behaviour / anti-bullying policy. More information on confiscation can be found in section 3.8 of the *School Discipline and Pupil Behaviour Polices* guidance [4]. School staff may request a pupil reveal a message or show them other content on their phone for the purpose of establishing if bullying has occurred, and a refusal to comply might lead to the imposition of a disciplinary penalty for failure to follow a reasonable instruction. Where the text or image is visible on the phone, staff can act on this. Where the school's behaviour policy expressly provides, a member of staff may search through the phone themselves in an appropriate case where the pupil is reasonably suspected of involvement.

---

[1] P. Smith, J. Mahdavi et al 2006

[2] www.msn.co.uk/customercare/protect/cyberbullying/default.asp?MSPSA=1

[3] www.teachernet.gov.uk/wholeschool/behaviour/schooldisciplinepupilbehaviourpolicies/

[4] www.teachernet.gov.uk/wholeschool/behaviour/schooldisciplinepupilbehaviourpolicies/

Legal duties and powers: Civil and criminal law

1.1.10 Although bullying is not a specific criminal offence in UK law, there are criminal laws that can apply in terms of harassment or threatening behaviour. For example – and particularly pertinent for cyberbullying – threatening and menacing communications.

1.1.11 In fact, some cyberbullying activities could be criminal offences under a range of different laws, including the Protection from Harassment Act 1997 which has both criminal and civil provision, the Malicious Communications Act 1988, section 127 of the Communications Act 2003 and the Public Order Act 1986. The age of criminal responsibility in the UK starts at 10.

- **Protection from Harassment Act 1997:** This Act is relevant for incidents that have happened repeatedly (i.e. on more that two occasions). Section 1 prohibits behaviour amounting to harassment of another. Section 2 provides a criminal offence and section 3 provides a civil remedy for breach of the prohibition on harassment in section 1. Section 4 provides a more serious offence of someone causing another person to fear, on at least two occasions, that violence will be used against them[5]. A civil court may grant an injunction to restrain a person from conduct which amounts to harassment and, following conviction of an offence under section 2 or 4, restraining orders are available to protect the victim of the offence.

- **Communications Act 2003:** Section 127 covers all forms of public communications, and subsection (1) defines an offence of sending a 'grossly offensive…obscene, indecent or menacing' communication[6]. Subsection (2) defines a separate offence where for the purposes of causing annoyance, inconvenience or needless anxiety, a person sends a message which that person knows to be false (or causes it to be sent) or persistently makes use of a public communications system[7].

- **Malicious Communications Act 1988:** Section 1 makes it an offence to send an indecent, grossly offensive or threatening letter, electronic communication or other article to another person with the intention that it should cause them distress or anxiety[8].

- **Public Order Act 1986:** Section 5 makes it an offence to, with the intent to cause harassment, alarm and distress, use threatening, abusive or insulting words, behaviour, writing, signs or other visual representation within the sight or hearing of a person likely to be caused harassment, alarm or distress[9]. This offence may apply where a mobile phone is used as a camera or video rather than where speech writing or images are transmitted.

- **Obscene Publications Act 1959:** It is an offence under this Act to publish an obscene article. Publishing includes circulating, showing, playing or projecting the article or transmitting that data, for example over a school intranet. An obscene article is one whose effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it[10].

---

5 www.opsi.gov.uk/acts/acts1997/1997040.htm

6 www.opsi.gov.uk/acts/acts2003/20030021.htm

7 Where cyberbullying occurs by messages transmitted via a public electronic communications network, it may amount to an offence under section 127(1) or (2). However, if the bullying is by means of a school intranet and the message is sent and received on the same school site, the message is unlikely to have been transmitted via the public network.

8 www.opsi.gov.uk/ACTS/acts1988/Ukpga_19880027_en_1.htm. This offence can be committed via an intranet which is not part of a public system.

9 www.opsi.gov.uk/si/si1987/Uksi_19870198_en_2.htm

10 Depravity and corruption are not confined to sexual depravity and corruption.

- When cyberbullying takes the form of hacking into someone else's account, then other criminal laws will come into play, such as the **Computer Misuse Act 1990** [11], in addition to civil laws on confidentiality and privacy.

- An anti-social behaviour order (ASBO) under the **Crime and Disorder Act 1998**[12] could be used for cyberbullying. An ASBO is a civil order which prohibits an individual from engaging in specific anti-social acts. An ASBO can be made against any person, aged 10 years or over, where there is evidence that their behaviour caused, or is likely to cause, harassment, alarm or distress to others and where an order is needed to protect person(s) from further anti-social acts. Whether a course of conduct is anti-social in nature is primarily measured by the consequences and the effect it has, or is likely to have, on a member or members of the community within which it is taking place. An ASBO can be used in conjunction with other measures as part of a tiered approach to tackling anti-social behaviour. Prohibitions should be precise, targeted at the specific behaviour complained of, and proportionate to the legitimate aim of protecting the community from further abuse. ASBOs can be extremely effective in preventing further escalation into criminal behaviour. Breach of an Anti-Social Behaviour Order is a criminal offence and criminal penalties apply.

- **Defamation:** Defamation is a civil "common law" tort in respect of which the Defamation Acts of 1952 and 1996 provide certain defences. It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet. A civil action for defamation can be brought by an individual or a company, but not by a public authority. It is up to the claimant to prove that the material is defamatory. However, the claimant does not have to prove that the material is false – the burden of proof on that point lies with the author/publisher, who has to prove that what they have written is true[13]. Where defamatory material is posted on a website the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in the jurisdiction, i.e. in England and Wales) obtain a court order (an injunction) to require removal of the material, and could sue either the host or the person who posted the material for defamation.

Cyberbullying in the school community

1.1.12 Cyberbullying is not a new phenomenon, but as mobile phone and internet use become increasingly common, so does the use of technology to bully.

1.1.13 Schools are already addressing bullying, discrimination and behavioural issues. This guidance on cyberbullying is designed to help school leaders and staff who may not be familiar with the ways in which technologies are currently being used by young people, and their potential abuse.

1.1.14 Taking a whole-school community approach, ensuring that the issues are discussed and the school community shares an understanding of what cyberbullying is and what the consequences and sanctions for it are, is key to effectively preventing and dealing with cases.

1.1.15 A lot of the material covered in this guidance is equally applicable to the cyberbullying of school staff as to pupils. Members of the school workforce

[11] www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
[12] www.opsi.gov.uk/acts/acts1998/19980037.htm
[13] www.opsi.gov.uk/acts/acts1996/1996031.htm

suffering from or concerned about cyberbullying can also contact their trade union or professional association for support and advice.

1.2 THE CONTEXT: YOUNG PEOPLE AND TECHNOLOGY

The role of technology in young people's everyday lives

1.2.1 Today's children and young people have grown up in a world that is very different from that of most adults. Subsequently, how young people use technology is not always understood by parents, carers and staff members.

1.2.2 Digital media, computers, mobile phones and the internet have been a taken-for-granted part of most children and young people's upbringing and environment. Many rely on technology not just to keep in touch, but as a way of developing their identities, socialising, and belonging to groups. Technology can play a positive, productive and creative part of young people's activities, development and social participation.

1.2.3 Engagement with technology involves feelings as well as actions – above all it is a social activity that allows young people to feel connected to their peers. Telling a young person who has been cyberbullied to keep their mobile phone switched off or to stay off the internet can be interpreted as a disruption of their social life and perceived as a punishment.

1.2.4 Barring or restricting school network access to particular sites that young people use, such as social networking and gaming sites, does not necessarily prevent young people from using them. They will still access them, via their own devices and connections, by bypassing blocks, or by finding new, unrestricted sites. Whatever policies and practices individual schools might have around computer access, mobile phones, or game consoles, it is important to recognise how important technology is to young people. Education and discussion around responsible use and e-safety is key to helping them deal confidently with any problems that may arise, whether in or out of school.

Adults are not always aware of how technologies can be used and abused

1.2.5 Teacher training is changing to incorporate and account for e-safety issues, and to equip new teachers with the information they need to make the most of technologies to support their learning and teaching practice. The Government's e-strategy supports ICT for continuing professional development for both teachers and leaders. Recently, Becta have become the Government's key partner in the strategic delivery and implementation of the strategy. There are many partner agencies working at national, regional and local level to support the best use and understanding of technology to support learning and teaching.

1.2.6 Technology constantly changes, and the pace of change can be off-putting for adults: new sites, crazes and fashions come and go continually. It may seem daunting or demanding of time that just isn't available to keep up with what young people are doing.

1.2.7 As technology develops, children will be experimenting with new environments and exploring where the boundaries of behaviour lie. In order to engage in a discussion about acceptable and responsible use, it is necessary to be informed about these technologies, in order to help identify where the limits are and what the potential impacts of certain behaviours are. It is not necessary to know about every application or site – but it is important to keep up to date with a broad understanding of the different ways that young people are using or abusing, technologies.

1.2.8 Understanding children and young people's online lives and activities can help adults respond to situations appropriately and effectively. Talking to students about what they do with technology, and

what their concerns and experiences are, is an essential starting point. Asking children and young people to show adults how technologies and services work is a useful strategy that can provide an important learning opportunity and context for discussing online safety.

1.3 FORMS THAT CYBERBULLYING CAN TAKE

1.3.1 Cyberbullying takes different forms, some of which are harder to detect or less obviously associated with bullying than others. Schools should already have policies and practices in place for dealing with some of these.

Threats and intimidation

1.3.2 Serious threats can be sent to both staff and pupils by mobile phone, email, and via comments on websites, social networking sites or message boards.

Harassment or stalking

1.3.3 Repeated, prolonged, unwanted texting, whether it is explicitly offensive or not, is a form of harassment. Online stalking (sometimes referred to as 'cyberstalking'), where a person's online activities are constantly monitored, can cause psychological harm and fear. Previously safe and enjoyable environments can be experienced as threatening, and online activity may become a source of anxiety.

1.3.4 Harassment and stalking can take several and often multiple forms online, and may or may not be a continuation of offline harassment or lead to physical harassment and stalking. Forms of harassment include:

- repeatedly sending unwanted text or instant messages, or making phone calls (including silent calls);
- using public forums, such as message boards or chatrooms, to repeatedly harass, or to post derogatory or defamatory statements in order to provoke a response from their target (sometimes referred to as 'flaming');
- tracking targets by using spyware;
- sending viruses.

Vilification / defamation

1.3.5 Cyberbullying can include posting upsetting or defamatory remarks about an individual online, or name-calling using a mobile device for example. These may be general insults, or include prejudice-based bullying. Pupils may use their mobile phones or email to send sexist, homophobic and racist messages, for example, or they may attack other kinds of difference – a physical or mental disability, cultural or religious background, appearance, or socio-economic position.

Ostracising / peer rejection / exclusion

1.3.6 Online exclusion can be harder to detect than children obviously being marginalised in a space, such as a classroom, where there are adults present.

1.3.7 Social networking sites, such as Bebo and MySpace, provide a platform for young people to establish an online presence and to talk with other network members. They can be an important extension of a young person's social space and activity. Most social networking sites work as gated communities, only allowing contact between members, so it is common for only a small number of social networking sites to be popular amongst any individual school's students. It is possible for a group of students to set up a closed group, which can protect them from unwanted contact. It also means that excluding someone – by refusing to return or acknowledge messages; deleting them from their friendship lists; or using 'ignore' functions – can be extremely hurtful.

Identity theft, unauthorised access and impersonation

1.3.8 'Hacking' generally means accessing someone else's account by finding out or guessing their username and password information. The majority of children and young people consulted (see 'What children and young people say' in the Resources section) during the production of this guidance were aware of such incidents.

1.3.9 Hacking into systems, accounts or files is not automatically a form of cyberbullying, but it is always a serious issue. Hacking is illegal under the Computer Misuse Act 1990 (see information on the civil and criminal law).

1.3.10 Examples of how hacking can be used to cyberbully include:

- Accessing and copying someone's information, for example emails or pictures, in order to harass or humiliate them. This could include posting private information on public sites, emailing or forwarding data by mobile phone, or printing and circulating paper copies.

- Deleting someone's information – for example, electronically submitted or stored assignments and homework, or important emails.

- Impersonating someone – for example pretending to be the person whose account has been hacked in order to post abusive comments and bad language. This might include posting messages to the school's Virtual Learning Environment (VLE), sending Instant Messages or emails, or may involve using someone's mobile phone to send abusive calls, texts or images. There have been cases where a bully has sent out nasty messages to everyone on a pupil's buddy list, and it can be difficult for the person targeted to make their friends believe the messages did not come from them. People have also discovered their images and contact details have been posted to public sites along with invitations to contact them.

1.3.11 You don't need to be able to access someone's account details to impersonate them. There are examples of people discovering websites, profiles or comments written in their name and pretending to be by them.

1.3.12 Identifying perpetrators using technology is often a time-consuming process, and it may not always be possible for the school to prove who the responsible party is (see 'Investigation' section of the 'Responding to cyberbullying' chapter). Identifying who has been cyberbullying may depend on more traditional ways of investigating incidents – circumstantial evidence, a witness report, or an admission of responsibility.

Publicly posting, sending or forwarding personal or private information or images

1.3.13 Once electronic messages or pictures are made public, containing them becomes very difficult. Video or pictures can be passed between mobile phones either by a local wireless connection (which allows free messages to be sent between devices that are close to each other), sent by text to other phones, uploaded to websites, or posted to public video-hosting sites. Most young people are aware of 'Happy Slapping', a term which has been used to refer to physical assaults that are recorded and circulated, usually via mobile phone. The DCSF does not promote the use of this term, although it recognises that its popular currency has at least allowed discussion around this form of cyberbullying to begin to take place. The term is inaccurate and misleading, and risks minimising serious and illegal incidents of physical assault. People who record attacks can be actively engaging in cyberbullying. Circulating images of attacks can also be a form of harassment, and will certainly compound the harm of the original attack.

1.3.14 Websites are potentially viewable by millions of people. Even after pages or comments have been removed, 'cached' copies may still be available. For example, Google creates a copy of the pages in its index which are stored as a cached version that can be accessed via its search results pages, unless a site owner has requested otherwise.

1.3.15 Creating, possessing, copying or distributing images of children and young people under the age of 18 which are of an indecent or sexual nature is illegal under the Protection of Children Act 1978. These images are illegal even if they were taken in 'fun' or by 'willing' parties. Section 160 of the Criminal Justice Act 1988 criminalizes the possession of electronic or hardcopy images. These laws also apply to indecent 'pseudo-photographs' – images which have not been taken but have been created or adapted, for instance using digital imaging software.

Manipulation

1.3.16 Manipulation is an often under-considered form of bullying, but unfortunately there have been many cases of manipulative cyberbullying. Examples include putting pressure on someone to reveal personal information or to arrange a physical meeting. This can be done by using online friendship status – for example, suggesting that a genuine friend would give out personal information.

1.3.17 It can be difficult to negotiate online relationships – some people will find using ignoring and blocking tools easy, others will hesitate to demote the status of people they have already thought of as friends. Manipulation is a very difficult type of cyberbullying to detect, since the person being bullied often feels implicated in and responsible for their own victimisation, and may feel guilty or ashamed. Some forms of manipulation may involve getting people to act or talk in a provocative way. Rude images or conversations can be very embarrassing to young people, and their fear that other people, including their family members, might find out can make them vulnerable to further manipulation. There is also evidence that mobile phones and the internet are being used to try to control, track and manipulate within abusive teen relationships[14].

1.3.18 Manipulation is also used by adults with a sexual interest in children to 'groom' children they have contacted online to meet up. This guidance concentrates on bullying and does not go into 'grooming' or wider child protection issues. For further information on this, see **www.ceop.gov.uk** or **www.chatdanger.com**.

1.4 HOW IS CYBERBULLYING DIFFERENT TO OTHER FORMS OF BULLYING?

Impact

1.4.1 In cyberbullying, the audience for the bullying can be very large and reached rapidly. This means that the degree and seriousness, as well as possible risks and repercussions, have to be evaluated differently than in cases of other types of bullying. If content is shared across mobile phones or posted online, it becomes difficult to control who might see it or have copies of it. Not being able to be certain that the event has been contained and will not recur / resurface may make it harder for the person being bullied to gain a sense of 'closure' over an event.

1.4.2 This is a particularly significant way in which cyberbullying is different from other forms of bullying: a single incident can be experienced as multiple attacks. For example, a humiliating video posted to the web can be copied to many different sites. A single instance of bullying – the creation of a nasty website or the forwarding of a personal email – can have repeated and long-term consequences, as content that is taken off the internet can reappear or be circulated again.

[14] Tech Abuse in Teen Relationships Study, January 2007: http://loveisnotabuse.com/pdf/06-208%20Tech%20Relationship%20Abuse%20TPL.pdf

1.4.3 It is also worth noting that some of those being bullied may not be aware that they have been or are being cyberbullied. For example, they may not have seen, or be aware of, content about them that has been posted online.

Targets and perpetrators

1.4.4 Children and young people are not the only ones that may be subject to cyberbullying. School staff have also been victimised and have suffered distress at the hands of school-aged bullies. The seeming anonymity and distance that technology provides means size and age are not necessarily relevant. People who cyberbully do not need to be physically threatening to cyberbully. They don't need to be stronger, taller or older than the person they are cyberbullying – they may never be in the same physical space as the person they are bullying.

1.4.5 Cyberbullying can be used by a person bullying offline to extend their aggression, but can equally be used as a form of 'revenge'. There have been some cases where the person cyberbullying had been previously bullied, and used the technology to respond.

1.4.6 Bystanders to cyberbullying can easily become perpetrators – by passing on or showing to others an image designed to humiliate another child or staff member, for example, or by recording an assault/act of bullying on a mobile phone and circulating this. As with other forms of bullying, it is important that the whole-school community understands their responsibility to report cyberbullying and support the person being bullied. It is advisable that anti-bullying policies refer to those 'bystanders' – better termed 'accessories' in this context – who actively support cyberbullying incidents and set out sanctions for this behaviour.

Location

1.4.7 Cyberbullying can take place at any time and can intrude into spaces that might previously have been regarded as safe or personal – the person being cyberbullied can be left feeling that there is no place to hide and that they might be attacked at anytime. Sending abusive text messages, for example, means that cyberbullying can take place any time of the day or night, and the target of the cyberbullying can be reached in their own home, even their own bedroom.

1.4.8 Traditionally, young people have been told to walk away from someone who is trying to bully them. However, it is not possible to walk away from constant phone messages or from a website which has been created to hurt you.

1.4.9 Cyberbullying will have an impact on the education and wellbeing of the person being bullied, and the physical location of the bully at the time of their action is irrelevant in this. Schools now have broad new powers to discipline and regulate the behaviour of pupils even when they are off the school site – these are set out in the Education and Inspections Act 2006 (see information on the law and also section 3.4 of the *School Discipline and Pupil Behaviour Policies* guidance[15]).

Anonymity

1.4.10 People who cyberbully may attempt to remain anonymous and this can be extremely disturbing for those that are being bullied. Although the person being bullied may know that their bully is from within their circle of friends or pupils at their school, they may not know the actual identity of the bully and this can make them uneasy, distrustful, and suspicious of all their relationships.

1.4.11 However, perpetrators are not as anonymous as they might think and there are ways of identifying cyberbullies. Having said that, although there is likely to be an evidence trail ('digital footprints') left by the

[15] www.teachernet.gov.uk/wholeschool/behaviour/schooldisciplinepupilbehaviourpolicies/

bully, finding out further information that might help identify who is responsible – by tracking down the person's email or IP address (their unique computer address) – is time consuming and usually requires the involvement of other agencies (the police and the service provider, for example). And in some cases, finding out this information will not clearly identify an individual. See the 'Responding to cyberbullying' section for further information.

Motivation for bullying

1.4.12 Some cyberbullying is clearly deliberate and aggressive. However, some instances of cyberbullying are known to be unintentional and the result of not thinking or a lack of awareness of the consequences. Online behaviours are generally less inhibited than offline behaviour, and some children report saying things to others online that they would not have done offline. Two other factors may be involved here:

- The distance between the bully and the person being bullied: The lack of context can mean that what might intended as a joke may not be received as such, and indeed may be deeply upsetting or offensive to the recipient. Additionally, because the bully cannot see the person being bullied, and the impact that their message has had, there is less chance for either to resolve any misunderstanding or to feel empathy.

- A single act can have unintended consequences: Sending a 'funny' (i.e. embarrassing or humiliating) picture of a fellow pupil (even a friend) to someone could be viewed as a one-off incident, but the nature of the technology means that the sender loses control of the image they have sent. It can be sent on, posted up online and have a wide circulation. For this reason, a one-off action can turn into a repetitive action, and have consequences for the person being bullied far beyond what the original sender may have anticipated.

1.4.13 Schools need to ensure that ignorance of the consequences and potential seriousness of cyberbullying is not a defence – that all pupils are aware of the issues and rules, for example through induction procedures, awareness days and Acceptable Use Policies (see the 'Preventing cyberbullying' section).

Evidence

1.4.14 Unlike other forms of bullying, many cyberbullying incidents can themselves act as evidence – in the form of text messages or computer 'screen grabs', for example. As well as evidence that an incident has taken place, they may also provide information about who the perpetrator is. A nasty text message, for example, will contain the message, the date and time that it was sent, and information about the phone it was sent from.

1.4.15 Having proof that they are being bullied might make it easier for some targets of bullying to come forward – however, a recent MSN report found that 74% of teens did not try to get help the last time they were cyberbullied[16]. Adults and young people may not know how important the evidence could be, or how to preserve it. You can find out more about preserving evidence in section 3.3 of the 'Responding to cyberbullying' chapter.

1.5 BRIEF INTRODUCTION TO THE TECHNOLOGY

Mobile phones

1.5.1 Children and young people use their mobile phones for much more than talking and texting. The most additional common uses include telling the time, downloading and forwarding pictures and film clips, checking email and accessing the internet, listening to music, and playing games. The wide range of activities phones are used for, coupled with the phone's role in managing young people's different social networks, makes the phone a powerful and important tool.

[16] www.msn.co.uk/customercare/protect/cyberbullying/default.asp?MSPSA=1

1.5.2 As well as being able to store music, take photos and video and send these to other phones, children can also share this content with other phones via short range wireless connections. Wireless personal area network technology uses radio waves, providing a free way for enabled devices (phones, computers, handheld game consoles) in close range of each other to share information.

Benefits

Mobile phones allow children to stay in touch with, and be contacted by friends and family, parents and carers. They can be useful in emergency situations, and they can allow children a greater sense of independence. They can be used for storing files, taking notes, capturing evidence, and research via an internet connection.

Risks

Supervising a young person's use of their mobile phone is far harder than, for example, their use of the family computer, since phones are rarely shared and potentially always on.

It is very easy for children to create and circulate content, including inappropriate content. Using a short range wireless connection, content can be sent for free between enabled devices. Once forwarded, content is almost impossible to control, and can easily spread by being passed on.

Mobiles and bullying

Mobiles have been used to cyberbully in a number of different ways: making nasty calls; sending nasty text messages; taking and sharing humiliating images; videoing and sharing acts of bullying and assault via camera phone (sometimes misleadingly called 'Happy Slapping', see note at 1.3.13). Content can be posted online or sent from phone to phone, or shared using a short range wireless connection between devices, bypassing the phone network altogether.

Instant Messenger and Voice Over Internet Protocols

1.5.3 Instant messenger (IM) is an application that allows the pupil to chat in real time (i.e. live) with people on a pre-selected friend/buddy list. IM programmes usually require you to download an application to your computer, although there are some web-based services available which do not need installing.

1.5.4 IM programmes let you see which of your contacts are online when you are, and let you chat using text while you are using your computer. Like social networking sites, IM services work between a network of people who have signed up to the same service and given each other permission to see and talk to each other when they are online. Unlike chatrooms, which are typically public and open to anyone signed up to the chat service, IM is more private, usually taking place between two people. Windows Live Messenger (previously called MSN Messenger) is a popular IM programme; however, there are several different types of IM services.

1.5.5 Voice Over Internet Protocols (VOIP) programmes are becoming increasingly popular since they offer unlimited free phone calls anywhere in the world, using an internet connected computer and microphone. Again, calls can only take place between people who have downloaded the same application. Services like Windows Live Messenger include IM, voice calling and video conferencing.

Benefits

Typically children use instant messenger as an extension of their regular social lives, to talk to friends outside of school. IM is a quick and effective way of keeping in touch, and is a good social tool. IM is also used by some teachers to keep in touch with students – in order to check through homework, for example. IM is extremely useful for some types of collaborative work and research. Some IM programmes keep records of IM conversations or at least offer this facility, which can be used as evidence of work or as an example of problem solving (it is a good idea to activate this function as it serves as the best evidence when making a report of cyberbullying).

Risks

Some Instant Messenger products can hold up to 600 'buddies', or contacts, and some children may see having as many 'friends' as possible as important. It is usually common for people with large buddy lists to know only a small proportion of the people on their list.

IM and bullying

Bullies can use IM to send nasty messages or content to other users. People can also 'hack' into IM accounts and send nasty messages to contacts.

Chatrooms and Message Boards

1.5.6 There are many chat sites online, hosted by major service providers such as AOL as well as by smaller independent websites. Typically chatrooms are thematically organised around interest, age, or location. Chatrooms allow groups of people from across the world to hold text (and sometimes voice) conversations in real time.

Benefits

Most chatrooms have a theme or topic, so it is possible to meet others from all around the world with the same interest as you and exchange ideas. Often people assume different identities in chatrooms, which means they can be free from real world stereotypes, such as age, race and appearance. For young people this can be an easy way to meet new people, or explore issues which they are too shy to talk about in person. Since many people can join in and observe a conversation at one time, chatrooms are very useful for collaborative work. Most chatroom programmes record conversations too.

Message boards allow different people to add replies to discussion topics, creating chains of replies around particular topics, which make take place over several months. Some message boards are moderated – no new messages will be published publicly until the owner reviews them – but many others are monitored only by users, who are expected to report any inappropriate messages.

Risks

Public chatrooms can be populated by anyone, since accounts usually only require an email address to verify a user's identity. Most chatrooms do not carry age verification; therefore children can visit chatrooms of an adult nature. People can behave inappropriately or abusively. The nature of chatroom exchanges tends to be less inhibited than when people meet in the real world for the first time, and children can be persuaded to give out too much personal information and contact details. Chatrooms are not necessarily moderated (by a person observing conversations as they happen) or monitored (by someone reviewing previous chat session transcripts). There have been cases of adults using public chatrooms to begin relationships with children and young people in order to sexually abuse them (see Resources section for educational and awareness materials in this and other internet safety areas).

Chatrooms and Message boards and bullying

Nasty or threatening messages can be sent, without the target necessarily knowing who they are from. Groups may ostracise and ignore individual children. Children and young people may be persuaded to give out private information, or enter into apparent friendships with people who are lying to them about who they are in order to develop a friendship which they later exploit.

Email

1.5.7 Email is now an essential part of most people's working lives. Email accounts are provided by schools, broadband providers or other internet companies.

Benefits

As well as the obvious communication benefits, web-based email addresses do not require external verification and such 'disposable' accounts can be extremely useful for entering competitions and other activities that generate unwanted or spam email.

Risks

Email can be used to send inappropriate images and to forward private information. Computer viruses and spam are common email hazards. Web-based email can also be used by people wanting to remain anonymous in order to send malicious or nasty mail.

Email and bullying

People can send bullying or threatening messages via email, or repeatedly send unwanted messages. Unsuitable images or video clips can be passed on. Personal emails can be forwarded inappropriately. The majority of computer viruses are forwarded by email.

Webcams

1.5.8 Webcams are small digital cameras which work with computers. They can be used to record photographs or video, which can then be posted on the internet or forwarded. Most commonly, they are used to see someone that you are talking to online.

Benefits

Webcams let you see, in real time (i.e. live), people you are chatting to, places or events. They can have educational value – they can bring far-off places to life; be used to view experiments; be used for video-conferencing; and be used to facilitate collaboration between schools in different parts of the country or the world. They can also help families to keep in touch with friends and relatives.

Risks

Children have been persuaded to take or send inappropriate photographs of themselves, either by their friends or by people they have only had contact with online. Webcam use can be difficult to supervise if the computer is in a child's bedroom or private space. Although fairly rare, there have been cases of people using virus programmes that can 'hijack' the output of a remote webcam and send the images to their own computers.

Webcams and bullying

Children can be persuaded or threatened into doing things on a webcam that they might not have otherwise done – undressing or acting in unsuitable ways, for example. Once someone else has content the child or young person would not like their parents to know about or be made public, they are at risk of being further manipulated or threatened.

Social network sites

1.5.9 Popular social networking websites such as MySpace and Bebo let users create their own homepages, set up 'blogs' and add friends.

1.5.10 Social network sites typically allow users to set up a profile page, listing their interests and other details, and they enable contact with other users. Many focus on interests or services – for example, photo storage and sharing (like Flickr), music preferences (like last.fm) or education (like EduSpaces). They may also provide 'blogging' or other website creation tools.

1.5.11 Social network sites are designed to help people find and make friends, and to make it easy to stay in touch.

Benefits

Young people use online space in much the same way that they use offline space – they socialise with friends and other people online, express themselves, and meet up in much the same way as they might do at youth clubs or shopping centres. These sites provide them with public and private space, and let them express themselves creatively by selecting and creating content. Young people can usually set permissions, giving them control over who can access their profiles and pages.

Risks

Many young people view the social network site they use as the hub of their online activity and will spend a lot of time on the look and content of their pages. Profiles and blogs may contain a lot of detailed and personal information – about themselves and their friends. This can be misused by bullies and sexual predators to gain information about an individual, their interests and tastes as well as their location or contact details. Children and young people often mistakenly view publicly available sites as private and personal places, and may post photographs for their immediate friends which may be inappropriate or embarrassing in other contexts. Sites which are not made private, or registered as belonging to an over 18 year old, are easy to search for and may be indexed and cached by search engines such as Google. Staff members and parents may view the time spent on social network sites as inappropriate and excessive, since many young people will check their sites several times a day for messages and to view their friends' activity.

Social networking and bullying

Social Network sites can be abused in a number of ways. Most allow comments to be left (although some sites enable users to review / approve content before it is shown), and nasty comments may be posted. People might use their own sites to spread rumours or make unpleasant comments about other people, or post humiliating images or video of them. Fake profiles are also fairly common, and these might be used to pretend to be someone else in order to bully, harass or get them into trouble.

Video-hosting sites

1.5.12 Images and video can be posted to blogs, social networking sites, and sent by email. There has been a tremendous rise in the popularity of video-hosting sites, such as YouTube, where clips are uploaded and shared. Popular video clips can be seen by hundreds of thousands of visitors to the sites, and clips are rated by viewers and comments (including video comments) can be posted about them. The video footage can also be embedded in other sites and pages.

Benefits

There can be a lot of good content to view on these sites – music videos, funny clips and other entertainment, as well as useful resources, including educational resources. Even internet safety and anti-bullying videos can be found on these sites. Video is stored on and streamed from the sites themselves, which means that viewing is very easy.

Risks

There are two ways that children may be exposed to risk on video-hosting sites: children may access inappropriate material (for example, violent or pornographic content), and they may post inappropriate material, which might make them contactable and vulnerable or which might lead to embarrassment of themselves or others.

Video-hosting and bullying

Video-hosting sites can be misused for cyberbullying, and staff as well as pupils have been victim to content posted up on such sites. The cyberbullying may take the form of video taken without the subject's knowledge, even from within class, that is then posted and shared, and/or acts of violence against people or property.

Virtual Learning Environments (VLEs)

1.5.13 Many schools now use software that creates a site especially designed for education, called a Virtual Learning Environment (or VLE). Programmes such as Moodle allow school staff to set assignments, tests and activities and to track their students' progress. A VLE might only be available from the school network, or might be accessible from any internet connection (i.e. from home).

Benefits

VLEs provide a structured way for staff to set work and deadlines, and for students to complete activities, submit assignments, and to communicate and collaborate with others from their school community. These sites are typically password protected, to enable closed working environments and to track the learners' progress through tasks. They can enable students to access resources from home.

Risks

If the site is accessible from any internet location, schools will want to ensure that a specific 'Acceptable Use Policy' is in place – although users are tracked, students need to be aware of appropriate and acceptable behaviour. It is also important that staff are aware of data protection issues, and how to respond to reports or discovery of offensive messages or images. Ensuring that passwords are kept private is important, so that accounts are not accessed or misused by anyone else.

VLEs and bullying

Although users are tracked, students may still misuse the platform or post inappropriate messages or images. VLEs usually consist of a range of tools – for example, message boards, chatrooms, and Instant Messaging – that can be misused in the same ways as services outside of the school environment. Hacking can provide a range of opportunities for cyberbullying – including sending nasty messages from someone's account, posting inappropriate comments, and deleting schoolwork.

Gaming sites, consoles and virtual worlds

1.5.14 A significant amount of the time young people spend using technology is taken up playing the wide variety of computer games that are available. Computer games can be accessed through online gaming sites, where chat between players across the world is facilitated, or on handheld consoles which use a wireless connection to enable people in the same location to play against each other or to message one another. Virtual worlds – 2 or 3D online sites where users are encouraged to design their own avatars (the figures that represent them in the virtual world), explore and create their own environments – are becoming increasingly popular.

Benefits

Gaming has been shown to help develop many positive skills – leadership and decision-making, puzzle solving, teamwork and collaboration. Games that involve physical movement (dance mats, for example) can provide children and young people with a fun way to exercise. There are now many ways of using game software within education – e.g. Wordshark, which is a collection of games designed to support students with dyslexia.

Virtual worlds can be used to explore and bring to life a range of topics – for example, recreating ancient cities or building virtual prototypes.

Risks

Many games are designed for the adult market and are inappropriate for children and young people, containing adult themes and explicit imagery, although games should carry labels which indicate the age they are appropriate for. Parents will often want to limit the amount of time spent on games, since completing levels and finishing will be fairly addictive in any effective game. Games and virtual worlds accessed online will be harder to monitor for appropriateness of content.

Gaming sites, consoles and virtual worlds and bullying

As with other programmes that allow people to communicate with one another, there have been instances of name-calling and abusive / derogatory remarks. Additionally, players may pick on weaker or less experienced users, repeatedly killing their character. Wireless-enabled consoles can be used to forward unwanted messages to other compatible devices.

2. Preventing cyberbullying

2.1 TAKING A WHOLE-SCHOOL COMMUNITY APPROACH

2.1.1 This section looks at prevention strategies and activities that are designed to support the whole-school community. By this, we mean learners, teachers, support staff, parents, school leaders, governors, and all the people who provide support – including teaching assistants, break and lunchtime supervisors, and extended school provision staff. Each activity should include a consideration of who can contribute to development, consultation and implementation, and how to best inform and involve as many people as possible. Some activities will be targeted at particular groups – however, effectively addressing cyberbullying means making sure the whole-school community knows that cyberbullying is not acceptable and knows how to identify and take action against cyberbullying.

2.1.2 Schools can take pro-active measures to help prevent cyberbullying from occurring, and to reduce the impact of any incidents that do happen. Schools are already required to have a clear policy on tackling all forms of bullying, which is owned, understood and implemented by the whole-school community. Cyberbullying prevention can build on this (see section 2.3 on reviewing and updating policies to include cyberbullying), promoting and maintaining a safe and welcoming environment as a responsibility and function of the whole-school community.

Co-ordinating responsibility

2.1.3 The first step is to decide who within the school community takes responsibility for the coordination and implementation of cyberbullying prevention and responding strategies. To be most effective, it is likely that the person nominated will be a member of the senior management team and/or the staff member responsible for coordinating overall anti-bullying activity. An effective approach requires clearly defined responsibilities, reporting lines and communication – essential in the context of the time and other resource challenges that staff have to manage. School staff with responsibility for pastoral care, behaviour and IT systems, as well as the school council, parents and teacher unions / professional associations representing staff, will need to work together.

2.1.4 It is useful to identify key partners from outside agencies who can support your school in tackling cyberbullying – the police, your Local Safeguarding Children Board, and a member of your local Broadband Consortia (if they are providing you with internet services) are recommended. Local Safeguarding Children Boards (LSCBs) play a key role

in coordinating and ensuring the effectiveness of work to safeguard and promote the welfare of children in their areas. Where instances of cyberbullying present a significant problem, and are considered a local priority for action, LSCBs may work with local authorities, schools and other organisations to support the development of effective policies to address the problem.

2.1.5 Sharing resources, practices and ideas with anti-bullying leads from other schools is also recommended. This can help ensure joined up and effective prevention planning and ensure that good practice is disseminated.

Case study:

Norfolk County Council have adopted a range of strategies for dealing with cyberbullying, focusing particularly on raising the awareness of adults who may not be aware of the potential for misuse of technology and the implications of this misuse. Among other things, Norfolk has: provided training for school staff and parents; organised a two-day conference for school staff on e-learning, including workshops on cyberbullying and e-safety; asked a group of young people to design assemblies on the topic of cyberbullying for primary and secondary schools for Anti-Bullying Week; and organised a conference for parents on the topic.

Preventing cyberbullying

2.1.6 There is no single solution to the problem of cyberbullying; it needs to be regarded as a live and ongoing issue. This section outlines a prevention framework made up of the five essential action areas that together offer a comprehensive and effective approach to prevention:

- Understanding and talking about cyberbullying
- Updating existing policies and practices
- Making reporting cyberbullying easier
- Promoting the positive use of technology
- Evaluating impact of prevention activities

2.1.7 The approach you take will reflect the culture, needs and preferences of your school community. However, your cyberbullying strategy will need to align with existing anti-discrimination work, curriculum delivery within Citizenship and PSHE, and the work you undertake as part of the Social and Emotional Aspects of Learning programme (SEAL) (see the general *Safe to Learn* guidance, in particular annex C, for more information on using the curriculum and the SEAL programme to address bullying).

2.1.8 As with other issues that potentially impact on the whole-school community, wherever possible and appropriate policies and processes should be discussed, agreed and developed collectively.

2.2 UNDERSTANDING AND TALKING ABOUT CYBERBULLYING

2.2.1 Cyberbullying is an issue that is already on your school's agenda. Cyberbullying prevention is an important way of working towards the Every Child Matters outcomes, and of safeguarding the health and wellbeing of your school community.

2.2.2 Developing and agreeing on a shared understanding of what cyberbullying is, and supporting school-wide discussion around the issue of cyberbullying provides a key foundation to all your prevention activities.

2.2.3 How can you make sure that the whole school is confident and clear in its understanding of cyberbullying?

Promote awareness and understanding about cyberbullying

2.2.4 It is important that the whole-school community has a shared, agreed definition of cyberbullying. All should be aware of the impact of cyberbullying and the ways in which it differs from other forms of bullying.

2.2.5 We advise that the whole-school community has an opportunity to contribute to and be a part of a policy and practice development and review discussion about cyberbullying.

2.2.6 As with other forms of bullying, it is vital to include discussion of prejudice-driven bullying. Sexist, racist and homophobic cyberbullying, as well as cyberbullying related to SEN and disabilities, should be addressed within any discussion and understanding.

Case study:
Mossley Hollins school in Manchester recently held a cyberbullying conference for their year 9 pupils – a whole day event including information, activities and workshops which focused on tackling cyberbullying. Following their work with the pupils, they invited parents to attend a one-hour information meeting (see item E in the Resources section for a copy of the letter to parents).

Publicising Sanctions

2.2.7 Pupils need to be aware of the importance of a safe environment and how to behave responsibly when using ICT. Pupils, parents, staff and governors should all be aware of the consequences of cyberbullying. Young people and their parents should be made aware of pupils' rights and responsibilities in their use of ICT, and what the sanctions are for misuse.

Case study:
Kesteven and Sleaford High School in Lincolnshire has produced information for learners and parents on sanctions for cyberbullying. You can review these for ideas about communicating your schools sanctions (see item F in 'Resources' section).

Provide information about out-of-school bullying

2.2.8 Under the Education and Inspections Act 2006, the school has new powers in relation to out-of-school bullying (see information on the law). Staff members and governors will need to understand what these are, so that they can deal with or refer cases appropriately. Students and parents will need to know that the school can provide them with support if cyberbullying takes place out of school.

2.3 UPDATING EXISTING POLICIES AND PRACTICES

2.3.1 This section deals with recording incidents, adapting existing policies and making sure everyone knows about any changes. Reviewing existing anti-bullying policies and school behaviour policies so that they cover cyberbullying incidents is an important part of your regular review of these documents. Cyberbullying issues will also impact on a range of other policies – staff development, ICT support and infrastructure, and e-learning strategies, for example.

Review and update policies to include cyberbullying

2.3.2 School governors, head teachers and senior managers should audit existing policies and procedures to decide which need to be changed or adapted in order to include cyberbullying prevention and how to respond to incidents.

2.3.3 The school's anti-bullying policy and/or school behaviour policy will certainly need to address cyberbullying if they do not already do so. It is important too that cyberbullying is addressed in ICT and other relevant lessons, and is brought to life through activities. As with other whole-school policies, it is important to include and empower young people to take part in the process.

Log all cyberbullying incidents

2.3.4 Keeping good records of any incidents of cyberbullying is essential, and can help to monitor the effectiveness of your school's prevention activities. The use of technology in any incident can be recorded using your existing incident report forms and these can be logged as cyberbullying incidents.

Review your existing Acceptable Use Policies (AUPs)

2.3.5 AUPs are the rules that students have to agree to follow in order to use ICT in school. If you only have these online, you might want to produce a paper form that can be sent home for parents to see. You may want to produce separate AUPs for using different kinds of technology – e.g. for use of the school network; use of a school Virtual Learning Environment (VLE) or other learning platforms / interactive tools; and use of mobile phones on school premises. Policies should outline the rules and responsibilities of use, sanctions for misuse, and issues around confiscation and retention.

2.3.6 It is for schools to decide if they wish to ban or restrict the use of mobile phones or certain internet sites during school hours. It is open for schools to include in their behaviour / anti-bullying policies measures to restrict the use of mobile phones and websites and strong sanctions for their misuse. Cyberbullying should be taken very seriously and schools should take such action as they consider appropriate to prevent it. However, it is important that such rules are well-publicised and that parents are aware of such measures (parents may currently contact their child via mobile to arrange suitable after-school collection times, for example, and need to know if phones will be required to be switched off during school hours) and that the school takes into account other implications as discussed in paragraph 1.2.4.

2.3.7 Staff who have a role in moderating and monitoring VLEs and other online environments should have clear guidance on how to respond to reports of cyberbullying or the discovery of offensive or upsetting material. If offensive material is posted on your institution's website, the school may face potential liability if they fail to take it down promptly once they are made aware of it. The AUP is a positive step the school can take towards ensuring material is not published, along with anti-cyberbullying and 'responsible use' activities. It is very important that action is taken as soon as the staff member responsible or the school becomes aware of any offensive material. Removing material needs to involve the school IT staff, since data may be required by a third party for investigation.

Case study:

An example of an Acceptable Use Policy for pupils from a secondary school in Manchester can be found in item H in the 'Resources' section. Pupils need to sign up to the policy to show both that they agree to the rules in the AUP and understand the consequences if they do not.

2.4 MAKING REPORTING CYBERBULLYING EASIER

2.4.1 Reporting any incident of bullying can be really hard for the person being bullied and for bystanders. You can read some of the reasons given for not reporting bullying in 'What children and young people say' in the Resources section.

2.4.2 It is important that adults in the community are aware of potential non-verbal signs and indications of cyberbullying. These include depression, anxiety, or fear. Staff should be alert to children seeming upset after using the internet or their mobile phone. This might involve subtle comments or changes in relationships with friends. They might be unwilling to talk or be secretive about their online activities and mobile phone use.

2.4.3 Making sure that all members of the school community recognise that asking for help from a person with greater authority is not a failing or a weakness, but a strength which shows good judgement. No one should feel that they have to deal with cyberbullying alone.

2.4.4 Because reporting can be difficult, it is important to have different ways for reporting cyberbullying incidents. Making reporting as easy as possible, and making sure everyone knows how they can report incidents is also an excellent way of raising awareness that cyberbullying is unacceptable.

Publicising school reporting routes

2.4.5 Schools are advised to provide parents and carers with information about cyberbullying policies, procedures and activities, and opportunities for becoming involved in these. This could be done in several ways – through an assembly or event which parents are invited to attend, through letters home and by posting information on the school website. Children, young people and parents will need information about all the ways they can report concerns and incidents and what they should expect to happen in return.

2.4.6 It is important to make sure that all staff, including support staff, know who they should talk to if they become aware of or suspect cyberbullying is taking place, and they understand how important reporting any cases can be.

Explore different reporting routes

2.4.7 There are a range of strategies, including pupil-centred strategies, which schools have successfully adopted to both raise awareness of bullying issues and offer pupils alternative reporting routes (see sections 4 and 5 of overarching *Safe to Learn* guidance).

2.4.8 Where peer support programmes are already in place, we advise that schools check what information is provided about cyberbullying and look at how cyberbullying can be included in training and awareness.

2.4.9 Setting up a cyberbullying taskforce, made up of pupils of all ages who are helped to identify what the problems are and develop solutions in conjunction with teaching staff, is a great awareness raising activity. It could also be carried out within existing groups – such as the school student council or an existing bullying or healthy schools student group.

Bystanders

Do not overlook the role and responsibility of bystanders. In cases of cyberbullying, bystanders or 'accessories' to the bullying have a more active role – they may forward on messages, contribute to discussions in a chat room, or take part in an online poll. So even though they may not have started the bullying or think of themselves as bullying, they are active participants, making the situation worse and compounding the distress for the person subjected to the bullying.

We know from talking to children that one of their biggest fears in reporting incidents they know about is that they will become the target of bullying. Schools can involve children and young people in developing 'bystander guidelines' that provide information about the responsibilities of bystanders in cyberbullying incidents.

Signpost information about external reporting routes

2.4.10 It may be appropriate to report incidents of cyberbullying directly to the internet service provider or mobile phone companies. There are websites that provide contact details[17] and schools can provide this information by letter to parents or from an area on their own websites. See our section on 'Responding to cyberbullying' for information on specific providers and technologies relating to reporting incidents, deleting accounts and getting offensive materials removed.

An example of one service provider:
"AOL offers bullying and general online safety advice on our Kids and Teens channels and younger AOL users can also speak to our agony aunt and uncle. In addition, we clearly signpost how users can report any inappropriate activity they come across. These reports are sent to AOL's Conditions of Service team, which reviews them and takes the appropriate action".

2.5 PROMOTING THE POSITIVE USE OF TECHNOLOGY

2.5.1 It is important for the adults in the school community to understand how children and young people think about and use technology. ICT is increasingly recognised as an essential life skill, and embedding technology across the curriculum and in learning and teaching delivery provides opportunities and benefits for both learners and staff members.

2.5.2 New technologies are being developed all the time, so keeping up-to-date and informed about young people's use of technologies, as well as their potential abuse and risks, is very important. While children and young people are experts on their own use and can be a valuable source of information about the technology, they may not necessarily understand all of the risks involved and the strategies for keeping their experience of technology safe and enjoyable (see 'Understanding cyberbullying' section).

2.5.3 Developing an organisational culture of confident ICT users supports innovation, e-safety and digital literacy skills, and helps to combat misuse and high-risk activities.

Review existing staff development targets and opportunities

2.5.4 Technology is successfully being used to support engaging, positive and effective learning, and to realise and increase the potential of personalised learning. The embedding of appropriate technologies within learning and teaching practice is a powerful tool which can be used to enhance learning opportunities for all – making learning more flexible, creative, accessible and engaging. Staff development around e-learning and technology provides a great opportunity for staff to both develop their own practice creatively and to support children and young people in their safe and responsible use.

2.5.5 As part of the performance management process line managers will be working with teachers to identify what professional development might help them develop their practice further. Where appropriate, schools should look at e-safety issues as an important component of technology for education for all members of the school community including school leaders and governors, as well as teachers, support staff and extended schools provision staff.

Promote e-safety and digital literacy

2.5.6 Explore safe ways of using technology with learners to support self-esteem, assertiveness, and participation and to develop friendships. Young people are more likely to report the misuse of technology in an environment where positive use is promoted.

[17] See, for example, www.stoptextbully.com.

2.5.7 Appropriate, safe and responsible behaviour in online environments may not be something that your learners have previously discussed or been supported in. Look at the ways in which you can support and discuss 'netiquette', e-safety and digital literacy.

2.5.8 Ensure that all staff and students are aware of the importance of keeping passwords confidential and user accounts secure. It is also important that everyone knows how to properly log out of accounts, and that students and staff members never leave logged in accounts unattended.

Password protection:

Everyone in the school community needs to understand the importance of keeping account information private and secure – for example, by using hard-to-guess passwords and changing them frequently. Children who have online accounts of any kind need to be aware that they should never share their passwords (exceptions here could include a parent or carer, teacher or ICT support staff member at school), and never let anyone use their accounts.

The school's Acceptable Use Policy (AUP) – the agreement between pupils and the school which outlines the responsibilities of learners using the school's computer network and equipment – may usefully refer to password privacy (see item H in the 'Resources' section for an example AUP). We also advise that it is covered in any internet safety lessons or induction to school accounts that might be password protected (e.g. the VLE).

2.5.9 Childnet International has produced a range of resources which can be used in the classroom or to support individual learners, staff members and parents:

- For Primary schools, see www.kidsmart.org.uk. For secondary schools, see www.childnet-int.org/kia/schools/.
- The SMART Rules – five rules for keeping in control of one's online activity. For Primary schools see www.kidsmart.org.uk/yp/smart/default; for secondary schools, see www.chatdanger.com/smart.
- For a resource for parents developed with the DfES (now DCSF), see http://www.childnet-int.org/kia/parents/.
- For a resource on online security developed by a young person for young people see www.childnet-int.org/sorted/.

Review how the school network is monitored

2.5.10 The ability to conduct searches of internet use records at school is an important part of being able to investigate incidents of cyberbullying (see 'Responding to cyberbullying' section). Your school may want to review and investigate available software, for example monitoring software and key logging programmes. It is important that learners are aware of what monitoring procedures are in place. Knowing that the school is taking such steps may also act as a disincentive for bullies to misuse school equipment and systems. However, it is important to remember that using technology to monitor, block or filter activity at school is only a partial solution.

2.6 EVALUATING THE IMPACT OF PREVENTION ACTIVITIES

2.6.1 Tackling cyberbullying is an ongoing process, and to get the most out of your prevention activities regular reviews of impact are vital. Cyberbullying should be included in your review processes, and included wherever appropriate in new policies. Monitoring your impact is an important way of marking and celebrating your school's progress.

2.6.2 The school should consider how it might most effectively measure the impact of prevention activities, and how it will communicate findings to the whole-school community. It is important to remember that when an issue is initially made visible and people feel safe to discuss and identify incidents, it is likely that the school will see the number of reports go up. It is important to communicate to parents and the whole-school community why this happens in the short term, and to recognise that reducing incidents is a longer-term goal.

Conduct a regular survey

2.6.3 The Children's Commissioner has recommended that all schools conduct an annual survey of pupil's experiences of bullying[18]. Cyberbullying incidents could be included in such a survey. This will provide schools with a good overview of how common cyberbullying incidents are amongst pupils, and highlight any areas that need particular attention. It will also provide you with a broad measure against which you can check the progress and impact of your prevention activities.

2.6.4 Many schools already use student and staff satisfaction surveys. It is useful also to conduct a parent satisfaction survey. Asking questions about cyberbullying will provide you with an indication about awareness and the success of your prevention work. The Anti-Bullying Alliance (ABA) Audit questionnaires are useful tools for evaluation[19].

Publicise progress and activities to the whole-school community

2.6.5 The staff members responsible for behaviour and anti-bullying can review cyberbullying prevention on an ongoing basis. Make sure you keep parents informed, by letter home and via the school website of your activities and the impact you are making.

---

[18] *Bullying Today: A report by the Office of the Children's Commissioner* (November 2006): www.childrenscommissioner.org/adult/consultationresponses.cfm?id=1920.

[19] www.anti-bullyingalliance.org.uk

3. Responding to cyberbullying

This section is designed to provide advice to schools on the options available for responding to incidents of cyberbullying.

3.1 CYBERBULLYING IS A FORM OF BULLYING

3.1.1 It is important to recognise that cyberbullying is a form of bullying, and as such schools should already be equipped to deal with the majority of cyberbullying cases through their existing anti-bullying and behaviour policies and procedures (see the 'Preventing cyberbullying' section for information on including cyberbullying in these policies).

3.1.2 In all cases of bullying, incidents should be properly documented, recorded and investigated; support should be provided for the person being bullied; other staff members and parents should be informed as appropriate; and those found to be bullying should be interviewed and receive appropriate sanctions.

3.1.3 There are particular features of cyberbullying that differ from other forms of bullying and need to be recognised and taken into account when determining how to respond effectively. The key differences are:

- Impact – the scale and scope of cyberbullying can be greater than other forms of bullying.
- Targets and perpetrators – the people involved may have a different profile to traditional bullies and their targets.
- Location – the 24/7 and anyplace nature of cyberbullying.
- Anonymity – the person being bullied will not always know who is attacking them.
- Motivation – some pupils may not be aware that what they are doing is bullying.
- Evidence – unlike other forms of bullying, the target of the bullying will have evidence of its occurrence.

For more information on the differences between cyberbullying and other forms of bullying, see section 1.4 of the 'Understanding cyberbullying' chapter).

3.1.4 Practices and procedures to report and respond to incidents of bullying and discrimination should already be in place in the school, and the majority of cyberbullying cases will be effectively dealt with within existing protocols.

3.1.5 In addition to existing procedures, staff should be particularly aware of the following during any response to cyberbullying incidents:

- Supporting the person being bullied
- Recording and investigating incidents
- Working with the bully and sanctions

3.2 SUPPORT FOR THE PERSON BEING BULLIED

3.2.1 As with other forms of bullying the target of cyberbullying may be in need of emotional support. Key principles here include reassuring them that they have done the right thing by telling someone; recognising that it must have been difficult for them to deal with; and reiterating that no-one has a right to do that to them. Refer to any existing pastoral support/procedures for supporting those who have been bullied in the school, and refer them to helpful information and resources (see section 4 of the overarching anti-bullying guidance, *Safe to Learn*).

3.2.2 Taking steps to ensure the school adopts a culture that does not tolerate cyberbullying can help to make the target of cyberbullying feel safe (see section on 'Preventing cyberbullying').

Advice on online empowerment

3.2.3 It is important to advise the person being bullied not to retaliate or return the message. Replying to messages, particularly in anger, is probably just what the bully wants, and by not replying the bully may think that the target did not receive or see the message, or that they were not bothered by it. Instead, the person should keep the evidence and take it to their parent or a member of staff (see section 3.3 on preserving evidence).

3.2.4 Advise the pupil to think about the information they have in the public domain and where they go online. It is important that pupils are careful about who they give their mobile phone number to, and that they consider whether they should stay members of chatrooms, for example, where people are treating them badly.

3.2.5 Advising the child to change their contact details, such as their Instant Messenger identity or mobile phone number, can be an effective way of stopping unwanted contact. However, it is important to be aware that some children may not want to do this, and will see this as a last resort for both practical and social reasons, and they may feel that they are being punished.

Try to contain the incident

3.2.6 Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. There are advantages in trying to contain the 'spread' of this. If bullying content, e.g. embarrassing images, have been circulated, it is important to look at whether this content can be removed from the web.

3.2.7 Some steps can be taken to try to stop it spreading:

- The quickest and most effective route to getting inappropriate material taken down from the web will be to have the person who originally posted it remove it. If you know who the person responsible is, ensure that they understand why the material is hurtful and ask them to remove it (see section 3.3 for advice on preserving evidence).

Quote from a parent:

"Thankfully my son's school were very helpful, they identified the child who posted the video from another video he had posted, they have disciplined the other child and had him remove the video, in fact they took the matter very seriously and also had any users who had posted anything with reference to the school remove their videos so that was very reassuring."

- Contact the host (e.g. social networking site) to make a report to get the content taken down (see 'When and how to contact the service provider' below). The material posted may breach the service provider's terms and conditions of use and can then be removed.

- Confiscation of phones containing offending content / asking pupils to delete the content and say who they have sent it on to. School staff can confiscate a mobile phone as a disciplinary penalty, and have a legal defence in respect of this in the Education and Inspections Act 2006 (s 94). However, staff do not have a right to search through pupils' mobile phones unless the school's behaviour policy expressly provides for this and the pupil is reasonably suspected of involvement in an incident of cyberbullying which is of a sufficiently serious nature (see section on Education Law for more information).

- Contact the police in cases of actual/suspected illegal content. The police will be able to determine what content is needed for evidential purposes, potentially allowing the remaining content to be deleted.

3.2.8 As previously stated, members of the school workforce, as well as pupils, have been bullied online, with insulting comments and material posted about them. This material should be dealt with seriously and incidents contained in the ways described above to ensure the well-being of staff.

Preventing recurrence (e.g. blocking or changing contact details)

3.2.9 There are some steps that the person being bullied can take, depending on the service that the bully has used, which can allow users to manage who they share information with and also who can contact them. These features can help a person being bullied to stop further contact from the person harassing them. For example, blocking the person from their email or instant messenger buddy list will mean that they will not receive messages from that particular sender anymore.

3.2.10 Pupils or their parents should be advised to contact the service provider or host (i.e. the chatroom, the social network provider, or mobile operator) to inform them of what has happened, and get their advice on how to stop this happening again. The service provider may be able to block particular senders or callers (for landlines), or advise on how to change contact details, and potentially delete the accounts of those that are abusing the service. This following section outlines what each service provider can do and gives details on how to contact them.

When and how to contact the service provider

Mobile phones

3.2.11 All UK Mobile operators have nuisance call centres set up and/or procedures in place to deal with such instances. The responses may vary, but possibilities for the operator include changing the mobile number of the person being bullied so that the bully will not be able to continue to contact them without finding out their new number. It is not always possible for operators to bar particular numbers from contacting the phone of the person being bullied, although some phone handsets themselves do have this capability. Action can be taken against the bully's phone account (e.g. blocking their account), only with police involvement.

3.2.12 Details of how to contact the phone operators:

- O2: 08705214000 or ncb@O2.com
- Vodafone: call customer services on 191 from a Vodafone phone or on any other phone call 08700700191 for Pay Monthly customers or on 08700776655 for Pay As You Go customers.
- 3: call 333 from a 3 phone, or 08707 330 333.
- Orange: call 450 on an Orange phone or 07973 100450 for Pay As You Go customers; call 150 from an Orange phone or 07973 100150 for Pay Monthly customers.
- T-Mobile: call customer services on 150 from your T-Mobile phone or on 0845 412 5000 from a landline, or email using the 'how to contact us' section of the T-Mobile website at www.t-mobile.co.uk.

Social networking sites (e.g. Bebo, MySpace, Piczo)

3.2.13 It is normally possible to block / ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site.

3.2.14 Many social network providers also enable users to pre-moderate any comments left on their profile before they are visible by others. This can help a user prevent unwanted or hurtful comments appearing on their profile for all to see. The user can also set their profile to 'Private', so that only those authorised by the user are able to access and see their profile.

3.2.15 It is good practice for social network providers to make reporting incidents of cyberbullying easy, and thus have clear, accessible and prominent reporting features[20]. Many of these reporting features will be within the profiles themselves, so they are 'handy' for the user. If social networking sites do receive reports about cyberbullying, they will investigate and can remove content that is illegal or breaks their terms and conditions in other ways. They may issue conduct warnings and they can delete the accounts of those that have broken these rules. It is also good practice for social network providers to make clear to the users what the terms and conditions are for using the service, outlining what is inappropriate and unacceptable behaviour, as well as providing prominent safety information so that users know how to use the service safely and responsibly.

3.2.16 Contacts of some social network providers:

- Bebo: reports can be made by clicking on a 'Report Abuse' link located below the user's profile photo (top left hand corner of screen) on every Bebo profile page. Bebo users can also report specific media content (i.e. photos, videos, widgets) to the Bebo customer services team by clicking on a 'Report Abuse' link located below the content they wish to report. Users have the option to report suspicious online activity directly to the police by clicking the 'Report Abuse' link and then clicking the 'File Police Report' button.
- MySpace: reports can be made via the 'Contact MySpace' link, which is accessible at the bottom of the MySpace homepage (http://uk.myspace.com/), and at the bottom of every page within the MySpace site.
- Piczo: reports can be made within the service (there is a 'Report Bad Content' button at the top of every member page). At the bottom of the home page and on the 'Contact Us' page there is a link to a 'Report Abuse' page. The 'Report Abuse' page can be found at http://pic3.piczo.com/public/piczo2/piczoAbuse.jsp.

[20] The Home Office are publishing good practice guidance for social networking providers, drawn up by social network providers, children's charities and others, see http://www.police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Instant Messenger (IM) (e.g. Windows Live Messenger or MSN Messenger)

3.2.17 It is possible to block users[21], or change Instant Messenger IDs so the bully is not able to contact their target any more. Most providers will have information on their website about how to do this. In addition, the Instant Messenger provider can investigate and shut down any accounts that have been misused and clearly break their terms of service. The best evidence for the service provider is archived or recorded conversations, and most IM providers allow the user to record all messages[22].

3.2.18 It is also good practice for Instant Messenger providers to have visible and easy-to-access reporting features on their service (see the Home Office good practice guidance for Instant Messenger providers[23]).

3.2.19 Contacts of some IM providers:

- MSN: when in Windows Live Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse' and there is also an online feedback form at http://support.msn.com/default.aspx?mkt=en-gb to report on a range of products including MSN Messenger.

- Yahoo!: when in Yahoo! Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse'.

E-mail providers (e.g. hotmail and GMail)

3.2.20 It is possible to block particular senders[24], and if the bullying persists an alternative is for the person being bullied to change their email addresses. The email provider will have information on their website about how to create a new account.

3.2.21 Contacts of some email providers:

- Hotmail: there is an online contact form at http://support.msn.com/default.aspx?mkt=en-gb.

- Gmail: there is an online contact form at https://services.google.com/inquiry/gmail_security4.

- Yahoo! Mail: there is a 'Help' link available to users when logged in, which contains a reporting form. This can also be seen at http://help.yahoo.com/l/uk/yahoo/mail/yahoomail/abuse/general.html?from_url=http://help.yahoo.com/l/yahoo/mail/yahoomail/abuse/abuse-15.html.

Video-hosting sites

3.2.22 It is possible to get content taken down from video-hosting sites, though the content will need to be illegal or have broken the terms of service of the site in other ways. On YouTube, perhaps the most well-known of such sites, it is possible to report content to the site provider as inappropriate. In order to do this, you will need to create an account (this is free) and log in, and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the video content itself.

3.2.23 YouTube provides information on what is considered inappropriate in its terms of service, see www.youtube.com/t/terms section 5C.

Chatrooms, individual website owners / forums, message board hosts

3.2.24 Most chatrooms should offer the user the option of blocking or ignoring particular users. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use. It is good practice for chat providers to have a clear and

[21] See www.chatdanger.com/messenger/safetyadvice_learn2.aspx

[22] See www.chatdanger.com/messenger/safetyadvice_learn.aspx

[23] See http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf?view=Binary

[24] See www.chatdanger.com/email/learn1.aspx

prominent reporting mechanism to enable the user to contact the service provider[25]. Users that abuse the service can have their account deleted.

Case study:
One young person was befriended by another player on a gaming site, who initially wanted to trade game items and was friendly. When the young person declined the trade, the other player became nasty and started threatening and swearing. The young person took a 'Print Screen' copy of the abusive text and blocked the other player to prevent any further contact. They also reported the players name and conduct to the game site administrator.

3.3 INVESTIGATION

Preserve the evidence

3.3.1 Schools should advise pupils and staff to try to keep a record of the abuse: particularly the date and time; the content of the message(s); and where possible a sender's ID (e.g. username, email, mobile phone number) or the web address of the profile / content. Taking an accurate copy or recording of the whole web-page address, for example, will help the service provider to locate the relevant content.

3.3.2 Keeping the evidence will help in any investigation into the cyberbullying by the service provider, but it can also be useful in showing what has happened to those who may need to know, including parents, teachers, pastoral care staff, and the police.

How to do this

3.3.3 It is always useful to keep a written record, but it is better to save evidence of bullying on the device itself:

- On mobiles, ensure the person being bullied keeps / saves any messages, whether voice, image or text. Unfortunately forwarding messages, for example to a staff member's phone, will result in information from the original message, such as the sender's phone number, being lost.

- On instant messenger, some services allow the user to record all conversations. The user could also copy and paste, save and print these[26]. When reporting to the service provider, or even to the police, copied and pasted conversations are less useful as evidence, as this can easily be edited. Conversations recorded / archived by the instant messaging service are better for evidence here. Conversations can also be printed out in hard copy or sections can be saved as a screen grab.

- On social networking sites, video-hosting sites, or other websites, keep the site link, print page or produce a screen grab of the page and save it. To take a copy of what appears on the screen, press Control and Print Screen, and then paste this into a word-processing document.

- On chatrooms, print the page or produce a screen grab of the page. To take a copy of what appears on the screen, press Control and Print Screen, and then paste this into a word-processing document.

- On email, ask the person being bullied to print it; forward the message on to the staff member investigating the incident; and encourage them to continue to forward and save any subsequent messages. Preserving the whole message, and not just the text, is more useful, as this will contain 'headers' (information about where the message has come from)[27].

[25] See http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf?view=Binary
[26] See www.chatdanger.com/messenger/safetyadvice_learn.aspx
[27] See www.fkbko.co.uk/EN.php?lang=EN&&subject=3&&id=43&&level=2

A note about images:

If images are involved in the cyberbullying, it is important to ascertain if these might be illegal or raise child protection concerns. Indecent or sexual images of children (defined as people under the age of 18) are illegal to produce, circulate or possess in the UK. These include images that children have taken of themselves or their friends, using their mobile phone for example.

Contact:

- Internet Watch Foundation, if the images are internet content (see www.iwf.org.uk).
- The local police if illegal images have been taken of a child and circulated.

Similarly if there is a recording of a crime, e.g. assault on another child, contact the local police.

If the images are not illegal or of an illegal act, then steps can be taken to try to contain the incident (see 'Try to Contain the Incident' above).

Identifying the bully

3.3.4 Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead to an identifiable individual. For instance, if another person's phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individual's phone or hacking into their IM or school email account to send nasty messages.

3.3.5 In cases where you do not know the identity of the bully, some key questions to look at:

- Was the bullying carried out on the school system? If yes, are there logs in school to see who it was? Contact the school ICT staff or ICT support to see if this is possible.
- Are there identifiable witnesses that can be interviewed? There may be children who have visited the offending site and left comments, for example.
- If the bullying was not carried out on the school system, was it carried out on a mobile or a particular internet service (e.g. IM or social networking site)? As discussed, the service provider, when contacted, may be able to take some steps to stop the abuse by blocking the aggressor or removing content it considers defamatory or breaks their terms of service. However, the police will need to be involved to enable them to look into the data of another user (see below).
- If the bullying was via mobile phone, has the bully withheld their number? If so, it is important to record the date and time of the message and contact the mobile operator. Steps can be taken to trace the call, but the mobile operator can only disclose this information to the police, so police would need to be involved. If the number is not withheld, it may be possible for the school to identify the caller. For example, another student may be able to identify the number or the school may already keep records of the mobile phone numbers of their pupils. Content shared through a local wireless connection on mobile phones does not pass through the service providers' network, and is much harder to trace (see 'Brief introduction to technology' section). Similarly text messages sent from a website to a phone also provide difficulties for tracing for the internet service or mobile operator.
- Has a potential criminal offence been committed? If so, the police may have a duty to investigate. Police can issue a RIPA (Regulation of

Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message. This may help to identify the bully. Relevant criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation (for example grooming or inappropriate sexual contact or behaviour). A new national agency called the Child Exploitation and Online Protection Centre (CEOP) was set up in 2006 to deal with child sexual exploitation, and it is possible to report directly to them online at www.ceop.gov.uk. However, it is important to note that it is the sexual exploitation of children and young people, not cyberbullying, which forms the remit of CEOP.

Information about cyberbullying and civil and criminal laws:

It is very important for schools to take cyberbullying seriously. It can be a very serious matter and can constitute a criminal offence. Although bullying or cyberbullying is not a specific offence in UK law, there are criminal laws that can apply in terms of harassment, for example, or threatening behaviour, or indeed – particularly for cyberbullying – threatening and menacing communications. See section on civil and criminal law for more detail.

Investigating allegations against staff

3.3.6 Some messages might allege abuse against a teacher or other member of staff. Online allegations should be handled in the same way as other allegations against staff, following the guidance in chapter 5 of *Safeguarding Children and Safer Recruitment in Education*[28]. The Department is currently reviewing its guidance on handling allegations against staff, and the issue of online allegations is being considered as part of this review.

3.4 WORKING WITH THE BULLY AND APPLYING SANCTIONS

3.4.1 Once the person responsible for cyberbullying has been identified, it is important that – as in other cases of bullying – sanctions are applied, and the range of sanctions include all those that are used in response to other forms of bullying.

3.4.2 Steps should be taken to change the attitude and behaviour of the bully, as well as ensuring access to any support that they may need.

3.4.3 When determining the appropriate response and proportionate sanctions, it is important to consider the ways in which cyberbullying incidents might differ in impact to other forms of bullying. The key considerations here may include attempts by the bully to disguise their identity; the public nature of posted material (and the extent of the humiliation); and the difficulty in controlling copies of the material (the difficulty in gaining closure over the event).

3.4.4 It should also be recognised, where induction and education activities are not in place, that some cyberbullying has been known to be unintentional or at least carried out with little awareness of the consequences. Determining appropriate sanctions for incidents will then require sensitivity to the impact on the person being bullied as well as any misunderstanding or thoughtlessness on the part of the cyberbully.

3.4.5 Consideration should also be given to the possibility that the cyberbullying could be a part of retaliation to previous bullying endured by the perpetrator.

[28] See http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DFES-04217-2006&

Sanctions for bullying behaviour

3.4.6 The aim of sanctions is to:

- Help the person harmed to feel safe again and be assured that the bullying will stop.
- Hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour.
- Demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly.

3.4.7 In addition to any sanctions that are in existing anti-bullying / behaviour policies, it is important to refer to any Acceptable Use Policy or agreement for internet and mobile use, and apply sanctions for breaches where applicable and practical.

3.4.8 Technology specific sanctions for pupils engaged in cyberbullying behaviour could include limiting internet access for a period of time or removing the right to bring a mobile phone into school (although issues of child safety should be considered in relation to the latter). For an example of how one school has technology specific sanctions, see item F in the 'Resources' section for a letter sent out to all the parents of one school outlining the sanctions that are in place.

3.4.9 For more information on disciplinary sanctions in general, see the *School Discipline and Pupil Behaviour Policies* guidance[29].

Working with the bully

3.4.10 It is important to ensure that the bully is helped to recognise the consequences of their actions, to help change their attitude, behaviour and the way they use technology. Effective steps can be taken here that reflect work done with other bullying behaviour, including measures like restorative justice. These are discussed in section 4 of the overarching *Safe to Learn* guidance.

[29] www.teachernet.gov.uk/wholeschool/behaviour/schooldisciplinepupilbehaviourpolicies/

CYBERBULLYING: Further resources

A. Key advice to parents and carers on cyberbullying

When a child is the target of cyberbullying – bullying via mobile phone or the internet – they can feel alone and very misunderstood. It is therefore vital that as a parent or carer you know how to support your child if they are caught up in cyberbulling. This short guide will help you.

1) PREVENT CYBERBULLYING

Where to start

The best way to deal with cyberbullying is to prevent it happening in the first place. Although it may be uncomfortable to accept, you should be aware that your child may as likely cyberbully as be a target of cyberbullying and that sometimes children get caught up in cyberbullying simply by not thinking about the consequences of what they are doing. It is therefore crucial that you talk with your children and understand the ways in which they are using the internet and their mobile phone. In this guide there is an anti-cyberbullying code which contains seven key messages for children, which you may find a helpful starting point for a discussion with them about issues, such as being careful about posting images on personal websites and where to go to get help.

Use the tools

Most software and services on the internet have in-built safety features. Knowing how to use them can prevent unwanted contact. For example, Instant Messenger services such as MSN Messenger have features which allow users to block others on their contact list and conversations can be saved on most Instant Messenger services. Social networking sites such as MySpace and Bebo also have tools available – young people can keep their profile set to 'private', for example, so that only approved friends can see it.

With bullies using text and picture messaging, it is also important to check with your children's internet or mobile phone provider to find out what protections they can offer, including whether it is possible to change your mobile number.

2) RESPONDING TO CYBERBULLYING

It is vital that you have strategies to help your child if they come to you saying that they are being cyberbullied.

The anti-cyberbullying code
Start by teaching your children the seven key messages in the anti-cyberbullying code (see item B). This includes advice on not replying or retaliating to cyberbullying, as well as not assisting a cyberbully by forwarding a message, even as a joke.

Keep the evidence
Keeping the evidence of cyberbullying is helpful when reporting an incident and may help in identifying the bully. This means keeping copies of offending emails, text messages or online conversations.

Reporting cyberbullying
There are a number of organisations that can help you if you need to report incidents of cyberbullying:

- **The school:** If the incident involves a pupil or pupils at your child's school, then it is important to let the school know. All schools have a legal duty to have measures in place to support the person being bullied and to apply disciplinary sanctions to the pupil doing the bullying. Schools are increasingly updating these policies to include cyberbullying.

- **The provider of the service:** Most service providers have complaints and abuse policies and it is important to report the incident to the provider of the service – i.e. the mobile phone operator (e.g. O2 or Vodafone), the instant messenger provider (e.g. MSN Messenger or AOL), or the social network provider (e.g. Bebo or Piczo). Most responsible service providers will have a 'Report Abuse' or a nuisance call bureau, and these can provide information and advice on how to help your child.

- **The police:** If the cyberbullying is serious and a potential criminal offence has been committed you should consider contacting the police. Relevant criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation, for example grooming, distribution of sexual images or inappropriate sexual contact or behaviour.

See item D for a list of useful websites and resources.

B. Key advice to children and young people on cyberbullying

ANTI-CYBERBULLYING CODE

Being sent an abusive or threatening text message, or seeing nasty comments about yourself on a website can be really upsetting. This code gives you seven important tips to protect yourself and your friends from getting caught up in cyberbullying and advice on to how to report it when it does happen.

1) Always respect others
Remember that when you send a message to someone you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone.

If you receive a rude or nasty message or picture about someone else, do not forward it. You could be assisting a bully, and even be accused of cyberbullying yourself. You could also be breaking the law.

2) Think before you send
It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a website. Remember that what you send can be made public very quickly and could stay online forever. Do you really want your teacher or future employer to see that photo?

3) Treat your password like your toothbrush
Don't let *anyone* know your passwords. It is a good idea to change them on a regular basis. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. Remember to only give your mobile number or personal website address to trusted friends.

4) Block the Bully
Most responsible websites and services allow you to block or report someone who is behaving badly. Make use of these features, they are there for a reason!

5) Don't retaliate or reply!
Replying to bullying messages, particularly in anger, is just what the bully wants.

6) Save the evidence
Learn how to keep records of offending messages, pictures or online conversations. These will help you demonstrate to others what is happening, and can be used by your school, internet service provider, mobile phone company, or even the police, to investigate the cyberbullying.

7) Make sure you tell
You have a right not to be harassed and bullied online.

There are people that can help:

- Tell an adult you trust, who can help you to report it to the right place, or call a helpline like ChildLine on 0800 1111 in confidence.

- Tell the provider of the service you have been bullied on (e.g. your mobile phone operator or social network provider). Check their websites to see where to report.

- Tell your school. Your teacher or the anti-bullying co-ordinator at your school can support you and can discipline the person bullying you.

Finally, don't just stand there – if you see cyberbullying going on, support the victim and report the bullying. How would you feel if no-one stood up for you?

C. What children and young people say

What did children and young people tell us about their experiences of cyberbullying?

During the consultation process, carried out while developing this guidance for schools, Childnet staff talked to primary- and secondary-aged pupils from London and Leicester about their views on cyberbullying. These views are included to give a young person's perspective on the issue of cyberbullying.

Many of the pupils had experienced cyberbullying personally, or had friends who had been cyberbullied. The vast majority of the children and young people used mobile phones and the internet on a regular basis. Most of them believed that they understood the technology better than their teachers and parents, and many reported helping teachers or parents with mobile phones and websites.

Reasons given for why young people might not tell someone they are being cyberbullied:

- They were scared of making the situation worse, for themselves or for other people.
- They had been threatened about what would happen if they did tell anyone.
- They felt ashamed about their own behaviour.
- If it was something rude, they often did not want to tell their mum – they felt too embarrassed to have conversations about things like that.
- They were worried it might be their fault and that they would also get punished, or that they had done something to deserve it.
- They were worried that grown-ups would not understand what had happened to them and that they would not be able to explain it properly.
- They were worried that grown-ups would be dismissive of cyberbullying because it 'was only words' and that their feelings would be dismissed as silly.

- They were scared that the person cyberbullying them might hurt them physically.
- They didn't know who to tell.
- They felt "closed up inside", and didn't know how to explain what was happening to them.
- They felt too depressed to be able to do anything about the cyberbullying.
- The thing they were being cyberbullied about was true and they didn't want everyone to know.
- They were being ganged up on by a group and were too scared to tell anyone.
- They were worried that adults would not believe them.

What did children and young people say they would do to help someone they knew was being cyberbullied?

Positive approaches:

- Some of the young people saw that supporting and befriending the victim was very important – making sure that the victim did not feel alone, talking through what had happened with them and trying to cheer them up. They identified that feeling isolated and depressed made positive action more difficult for the person involved.
- Nearly all the children and young people recognised that telling someone with more authority than them would be the best way to help the victim. They named a range of people, including the police, teachers, grown-ups they liked, their parents, and their head teacher.
- In some cases they felt safer contacting expert groups – they talked about phoning ChildLine, and also emailing Childnet International.
- Many of the children said that they would report what had happened to the people running the website or to the phone company.
- Giving advice to the person being cyberbullied was seen as a useful thing that they could do – this included telling the person being bullied not to reply or get involved; to save any messages; and to take 'print screen' images for evidence.

Approaches to be cautious of:

- Some children and young people said that they would take responsibility for sorting the problem out themselves directly. This included talking with the person doing the cyberbullying and trying to get them to see what they were doing was wrong.
- Some young people suggested passing the problem on to older brothers and sisters to sort out.

Young people need to know that they are not expected to sort out problems on their own, but that they will be helped and supported by adults.

Dangerous Approaches:

- Some children and young people said that they would cyberbully the person back, or beat up the person doing the cyberbullying.
- Others said that they would do nothing – they would be too scared of being bullied themselves to get involved.

D. Useful websites and resources

Research

- Research by Nathalie Noret (York St John) and Professor Ian Rivers (Queen Margaret's University Edinburgh), 2007[30].
- Research carried out for the Anti-Bullying Alliance (ABA), *Cyberbullying: its forms and impact in secondary school pupils* by P. Smith, J. Mahdavi et al, 2006[31].
- MSN cyberbullying report, 2006[32].
- UK Children Go Online study by Sonia Livingstone and Magdalena Bober (LSE), 2005[33].

Helplines

- Childline – free 24 hour helpline for children and young people. Tel: 0800 1111.
- Kidscape – run a telephone advice line exclusively for parents and carers giving advice about bullying. Tel: 08451 205 204 (10am-4pm weekdays).
- Get Connected – free confidential helpline for young people (open 1pm-11pm every day). Tel: 0808 8084994.
- Samaritans – helpline for those in distress, offering multi-channel support. Tel: 08457 90 90 90. Email: Jo@samaritans.org. SMS text: 07725 909090.

Useful websites:

- **Childnet** – a range of resources for primary and secondary schools, for children and young people, for teachers and for parents (www.childnet-int.org).
- **StopText bully** – a website dedicated to mobile phone bullying, contains advice for young people including how to contact your operator (www.stoptextbully.com).

[30] See http://www2.yorksj.ac.uk/default.asp?Page_ID=4330
[31] See http://www.dfes.gov.uk/research/data/uploadfiles/RBX03-06.pdf
[32] See http://www.msn.co.uk/customercare/protect/cyberbullying/default.asp?MSPSA=1
[33] See http://www.children-go-online.net

- **Cyberbullying.org** – one of the first websites set up in this area, for young people, providing advice around preventing and taking action against cyberbullying. A Canadian-based site (www.cyberbullying.org).

- **Chatdanger** – a website that informs about the potential dangers online (including bullying), and advice on how to stay safe while chatting (www.chatdanger.com).

- **Anti-Bullying Alliance** – the Alliance brings together over 60 organisations into one network with the aim of reducing bullying. Their website has a parents section with links to recommended organisations who can help with bullying issues (www.anti-bullyingalliance.org.uk).

- Many of the internet service providers, mobile phone companies and social networking sites have useful advice and safety tips for users and parents on their own websites.

- **Please see section I of the 'Resources' section in *Safe to Learn*, the over-arching anti-bullying guidance, for more organisations that can help.**

Internet safety resources

- For more information on policies around ICT in schools, including Acceptable Use Policies (AUPs) for staff and pupils, see www.becta.org.uk/schools/esafety.

- The Child Exploitation and Online Protection Centre (CEOP), has produced a set of resources around internet safety for secondary schools called Think U Know, see www.thinkuknow.co.uk. CEOP also provide resources and training in delivering the Think U Know presentation in schools.

- Childnet International have a range of resources for primary and secondary schools. The website also has a sample family agreement which can be printed out (see www.childnet-int.org/kia/parents – click on see sample content from Know IT All for Parents).

Good practice guidance

For the providers of internet services:

- The Home Office are publishing good practice guidance for social networking providers, drawn up by social network providers, children's charities and others[34].

- The Home Office have already published such guidance for chat, instant messenger and web-based services providers[35]. And on moderating interactive services[36]. These good practice guidance documents contain a range of recommendations for service providers, including around education of their users; making reporting an easy and prominent facility for users; and providing tools for their users (such as blocking tools).

For UK mobile operators:

- *UK code of practice for the self-regulation of new forms of content on mobiles*[37]. This code outlines the mobile operators commitment to deal vigorously with malicious communications.

[34] see http://www.police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce.
[35] see http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf?view=Binary
[36] See http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation.pdf?view=Binary
[37] See www.imcb.org.uk/assets/documents/10000109Codeofpractice.pdf

E. Case study: letter inviting parents to cyberbullying information event

Dear Parent/Carer,

CYBER BULLYING PARENTS' INFORMATION EVENING – TUESDAY 6TH MARCH 2007

Cyber Bullying is a form of bullying that is on the increase nationally. It is where a child is tormented, threatened, harassed, humiliated, embarrassed or targeted by another child using the Internet, mobile phone, or other type of digital technology. We do not have any specific concerns in relation to our own school, but we do want to ensure that issues faced by children nationally are addressed.

Both the local education authority and the Cyberspace Research Unit (CRU) at the University of Central Lancashire have encouraged our school to take a lead in this area, given their view of our strong record on anti-bullying thus far.

With this in mind, we are holding an intensive full day ***Cyber Bullying Conference*** for all of our Year 9 pupils in school on Wednesday, March 7th. During the four sessions, the students will be given valuable information about how to deal with this type of bullying as well as being able to participate in workshops covering various aspects of this unacceptable behaviour.

As Mossley Hollins is pioneering this type of event, representatives of Childline, Childnet, UCLAN, DfES and Tameside MBC will be joining us on the day to share their expertise. Nationally, it has been noted that much of this type of bullying occurs in the home via mobile phones and the internet and so it is vital that you, as parents, are informed and aware of what steps you can take to prevent any such problem. **Therefore, we would like to invite you (no students) to attend an information giving evening on Tuesday, 6th March in the School Arts Theatre at 6:30pm.**

We expect that this meeting will last for approximately one hour, but we really feel that it will be an hour well spent and of great value.

Please make every effort to attend this meeting and we would be grateful if you could complete the attached reply slip.

Thank you as always for your support.

Head of Upper School/Deputy Head of Year 9

I/we will/will not be attending the Cyber Bullying Information Meeting at 6:30pm on Tuesday 6th March. Please return by Friday, 2nd March.

Refreshments will be provided.

Signed _____

Parent/Carer of _____ Form _____

F. Case study: information letter on sanctions

Kesteven & Sleaford High School

Dear Parents/Guardians

As you may already know, as part of our procedures for monitoring unsafe activity on the internet and by email, and in order to promote responsible computer use, the school monitors its network using a monitoring software product. This system allows all student activity on our network to be monitored and inappropriate use to be identified.

Use of this product has dramatically reduced instances of abuse on our network. However, when inappropriate use occurs, the school has a framework of sanctions as outlined below:

Internet abuse: 2-4 weeks limited internet access, depending on the severity of the abuse.

Email abuse: 2-4 weeks withdrawal of email privileges, depending on severity.

Network abuse: 2-4 weeks limited access or total withdrawal depending on the severity.

Please note these sanctions have been designed so that they will not impact on the education of our students. Limited internet access status confines the internet access to a predefined list of websites needed for their studies. This list is maintained by department heads and is updated on a regular basis.

In serious instances a copy of the incident is sent home with an accompanying letter.

Although these incidents are a rarity, this framework of sanctions, accompanied in each case by an interview with a member of the pastoral team, provides an opportunity to reinforce a responsible use ethic that will prepare pupils for ICT use outside the school environment.

The school is happy to answer any questions about this policy, so please feel free to contact us if there is anything you would like to discuss.

G. Case study: example acceptable use policy

Mossley Hollins High School

Information and Communications Technology
Acceptable Use Policy

Pupil Guidelines for Internet Use

General

Pupils are responsible for good behaviour on the internet just as they are in a classroom or a school corridor. General school rules apply.

The internet, primarily, is provided for pupils to conduct research and backup their work. Parents/carer's permission is required before a pupil is granted access. Access is a privilege, not a right and that access requires responsibility.

Individual users of the internet are responsible for their behaviour and communications over the network. Users must comply with school standards and honour the agreements they have signed.

Computer storage areas (including any external storage media you bring to school) will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private.

During school, teachers will guide pupils towards appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted within the school environment:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws.
6. Using others' passwords or accounts
7. 'Hacking' into others' folders, work or files for any reason.
8. Intentionally wasting limited resources, including printer ink and paper.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on internet/computer use.
2. Your parents/carers will be informed.
3. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
4. When applicable, police or local authorities may be involved.
5. If necessary, external agencies such as Social Networking or Email Member sites may be contacted and informed.

Pupils

- You must have your parent's / carer's permission before using the internet.
- You must have a supervising teacher or member of staff with you at all times when using the internet.
- Do not disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- Do not upload/send personal addresses, telephone / fax numbers or photographs of anyone (*staff or pupil*) at the school.
- Use of names of pupils, or photographs of students will require parents to have been informed about such use.
- Do not download, use or upload any material which is copyright. Always seek permission from the owner, before using any material from the internet. If in doubt, do not use the material.
- Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material of a violent dangerous or inappropriate context. If you are unsure ask the supervisor.
- Always respect the privacy of files of other users.
- Be polite and appreciate that other users might have different views than your own. The use of strong language, swearing or aggressive behaviour is not allowed. Do not state anything which could be interpreted as libel.
- Ensure that you have followed the correct procedures for using the internet.
- Report any incident which breaches these rules to the I.T. Network Manager or Co-ordinator of ICT.

I have read and agree to abide by the rules stated in the I.C.T. Acceptable Use Policy. I understand the consequences if I do not.

Name: _____ Form: _____

Signed: _____ Date: _____

You can download this publication or order copies online at
www.teachernet.gov.uk/publications

Search using the ref: DCSF-00658-2007

Copies of this publication can also be obtained from:

DCSF Publications
PO Box 5050
Sherwood Park
Annesley
Nottingham NG15 0DJ
Tel: 0845 60 222 60
Fax: 0845 60 333 60
Textphone: 0845 60 555 60

Please quote ref: 00658-2007DOM-EN

ISBN: 978-1-84775-028-0

PPBEL/D21/0907/53

Crown Copyright 2007

Extracts from this document may be reproduced for non-commercial research, education or training purposes on the condition that the source is acknowledged. For any other use please contact **hmsolicensing@opsi.x.gsi.gov.uk**

75% recycled
This publication is printed on 75% recycled paper

recycle
When you have finished with this publication please recycle it

department for
children, schools and families