Llywodraeth Cymru
Welsh Government

www.cymru.gov.uk

Respecting others: Cyberbullying

Guidance

Guidance document No: 057/2011
Date of issue: September 2011

Respecting others: Cyberbullying

Audience Schools, local authorities, parents/carers, families, learners and school governors; social workers, health professionals and voluntary organisations involved with schoolchildren.

Overview This guidance provides information for all involved in tackling bullying in schools. Local authorities and schools should find it useful in developing anti-bullying policies and strategies, and responding to incidents of bullying. This document forms part of a series of guidance materials covering bullying around race, religion and culture; bullying around special educational needs and disabilities; sexist, sexual and transphobic bullying; and homophobic bullying.

Action required For use in developing anti-bullying policies and strategies.

Further information Enquiries about this guidance should be directed to:
Pupil Engagement Team
Welsh Government
Cathays Park
Cardiff
CF10 3NQ
Tel: 029 2080 1445
Fax: 029 2080 1051
e-mail: PETshare@wales.gsi.gov.uk

Additional copies This document is only available on the Welsh Government website at www.wales.gov.uk/educationandskills

Related documents *Respecting Others: Anti-Bullying Guidance* National Assembly for Wales Circular 23/2003 (2003)
National Behaviour and Attendance Review (NBAR) Report (2008)
Inclusion and Pupil Support National Assembly for Wales Circular 47/2006 (2006)
School-based Counselling Services in Wales (2008)
School Effectiveness Framework (2008)

ISBN 978 0 7504 6239 6

WG12194
F8941011

Contents

Introduction

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

This guidance forms part of the Welsh Government's series of anti-bullying guidance materials for schools. Other guidance in the series includes:

- anti-bullying overview
- bullying around race, religion and culture
- bullying around special educational needs and disabilities
- homophobic bullying
- sexist, sexual and transphobic bullying.

This guidance is aimed at all maintained primary and secondary schools in Wales, including maintained special schools and pupil referral units. Increasingly schools are expected to work in partnership with a range of other agencies, organisations and bodies who may also find this guidance useful.

Terminology

For ease of reading, the term 'children' is used to mean 'children and young people' throughout the text. The definition of a 'parent' or 'carer' for the purpose of this guidance is broadly drawn and includes any person who has parental responsibility (which includes the local authority where they have a care order in respect of the child) and any person (for example, a foster carer) with whom the child lives and/or the child's birth parent(s).

Information on bullying in general can be found in the following documents.

- *Respecting Others: Anti-Bullying Guidance* National Assembly for Wales Circular No: 23/2003 which includes schools policies, definitions and strategies www.wales.gov.uk/respectingothers
- *Evaluation of Anti-Bullying Policies in Schools in Wales* commissioned by the Welsh Assembly Government in 2006 www.wales.gov.uk/topics/educationandskills/schoolshome/wellbeing/antibullying/publications/evaluationbullyingschools/?lang=en

- *Tackling Bullying in Schools: A survey of effective practice* published in 2006 by Estyn
  www.estyn.gov.uk

Section 1: Understanding cyberbullying

Schools know how to prevent and respond to bullying, and will already have strategies in place. Preventing and responding to cyberbullying should be part of these existing strategies.

This guidance helps with the specifics of dealing with cyberbullying.

> 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.

(13-year-old learner)

Cyberbullying is not a new phenomenon, but as the use of the internet, mobile phones and other portable devices become increasingly common, so does the use of technology to bully. Schools are already addressing bullying, discrimination and behavioural issues. This guidance is designed to help school leaders and staff who may not be familiar with the ways in which technologies are currently being used by learners and their potential abuse.

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

(Secondary school teacher)

A lot of the material covered in this guidance is equally applicable to the cyberbullying of school staff as it is to learners. Members of the school workforce suffering from, or concerned about cyberbullying, can also contact their trade union or professional association for support and advice.

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

(Parent)

Defining cyberbullying

Cyberbullying can be defined as the use of information and communication technology (ICT), particularly mobile phones and the internet (including social networking sites, blogs, e-mail, video and instant messaging), to deliberately upset someone else.

The Anti-Bullying Alliance defines it as:

> '. . . an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who can not easily defend him or herself.' (www.anti-bullyingalliance.org.uk)

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.

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, sexist 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.

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. These differences are important ones for people working with children and young people to understand.

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.

> One of my staff members was recently the victim of cyberbullying – some of the learners created a website 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 the episode nearly destroyed this man.
>
> (Headteacher)

The context – young people and technology

The role of technology in young people's everyday lives

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

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.

Engagement with technology involves feelings as well as actions – above all it is a social activity that allows children and 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.

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, through 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

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. 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.

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.

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.

Understanding children and young people's online lives and activities can help adults respond to situations appropriately and effectively. Talking to children and young people 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.

Forms that cyberbullying can take

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

Serious threats can be sent to both staff and learners by mobile phone or e-mail, or by comments on websites, social networking sites or message boards.

Harassment or stalking

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.

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

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. Learners may use their mobile phones or e-mail 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

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

Social networking sites such as Facebook, 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 among any individual school's learners.

Although most social networking sites enable a profile to be set to 'private' and only viewed by approved contacts, many users do not apply them. Maintaining very detailed online profiles, including personal information, photos and accounts of daily routines can lead to users being identified or contacted in person.

It is possible for a group of learners 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, blocking contact by deleting them from their friendship lists, or using 'ignore' functions – can be extremely hurtful. Most social networking sites set age restrictions on using their services, but there is no way of authenticating users. As a result many younger children disregard the terms and conditions of the service, unaware of the risks this might pose.

Identity theft, unauthorised access and impersonation

'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 during the production of this guidance were aware of such incidents.

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).

Examples of how hacking can be used to cyberbully include:

- accessing and copying someone's information, for example e-mails or pictures, in order to harass or humiliate them – this could include posting private information on public sites, e-mailing or forwarding data by mobile phone, or printing and circulating paper copies
- deleting someone's information, e.g. electronically submitted or stored assignments and homework, or important e-mails
- 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 e-mails, 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 learner'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.

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. 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 'Recording and investigating cyberbullying incidents' on page 48). 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

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 by mobile phone. 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.

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.

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 criminalises 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, by using digital imaging software.

Manipulation

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.

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.

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

How is cyberbullying different to other forms of bullying?

Impact

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.

This is a particularly significant way in which cyberbullying is different from other forms of bullying. 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 e-mail – can have repeated and long-term consequences, as content taken off the internet can reappear or be circulated again.

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

Targets and perpetrators

Children and young people are not the only ones who 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 necessarily need to be physically threatening. 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.

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.

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

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.

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. Cyberbullying will have an impact on the education and well-being 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 powers to discipline and regulate the behaviour of learners even when they are off the school site – these are set out in the Education and Inspections Act 2006. Revised guidance for schools covering the behaviour and conduct of learners outside schools was issued by the Welsh Assembly Government in October 2010. For more information, see www.wales.gov.uk/topics/educationandskills/schoolshome/pupilsupport/inclusionpupilsupportguidance/?lang=en

Anonymity

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 learners 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.

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 bully, finding out further information that might help identify who is responsible – by tracking down the person's e-mail 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). In some cases, finding out this information will not clearly identify an individual (see Section 4 'Responding to cyberbullying' on page 42 for further information).

Motivation for bullying

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 and young people 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 be intended as a joke may not be received as such, and 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 learner (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 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 that which the original sender may have anticipated.

Schools need to ensure that ignorance of the consequences and potential seriousness of cyberbullying is not a defence – that all learners are aware of the issues and rules, for example, through induction procedures, awareness days and acceptable use policies.

Evidence

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.

Having proof that they are being bullied might make it easier for some targets of bullying to come forward. However, an MSN report in March 2006 found that 74 per cent of teenagers did not try to get help the last time they were cyberbullied. Adults and young people may not know how important the evidence could be, or how to preserve it.

The level of cyberbullying in Wales

A *Survey into the Prevalence and Incidence of School Bullying in Wales* (Welsh Assembly Government, 2010) indicated the following.

- 17 per cent of learners in Year 6, 15 per cent of learners in Year 7 and 11 per cent of learners in Year 11 reported experiencing cyberbullying in the last two months (through one or more of social networking websites, using mobile phones and using e-mail).

- Bullying using social networking websites was consistently higher than the other forms of cyberbullying.
- Girls are more likely to be involved in cyberbullying. For example, in Year 7, girls were three times more likely than boys to report being bullied through social websites (16 per cent of girls compared to 5 per cent of boys).
- The decline in the percentage of learners experiencing cyberbullying as learners get older is small compared to other forms of bullying.

However, the survey indicates that the types and locations of bullying which have traditionally been common remain the most widespread across all year groups. Newer forms of bullying, such as cyberbullying, while not insignificant, are much less prevalent. The main and summary reports are available at www.wales.gov.uk/topics/educationandskills/publications/researchandevaluation/research/surveyschoolbullying/?lang=en

Other research on the levels of cyberbullying

A 2010 study of 4,000 young people between the ages of 12 and 18 from a large school district in the southern United States indicated the following.

- 17 per cent reported experiencing cyberbullying in past 30 days. When asked about specific types of cyberbullying in the previous 30 days; mean or hurtful comments (13.7 per cent) and rumours spread online (12.9 per cent) continue to be among the most commonly cited.
- Approximately 20 per cent admitted to cyberbullying others in their lifetimes. Posting mean or hurtful comments and spreading rumours online were the most commonly reported types of cyberbullying (see www.cyberbullying.us/research.php).
- Research carried out for the Anti-Bullying Alliance in 2007 found that 22 per cent of 11 to 16-year-olds had experienced cyberbullying.
- The MSN cyberbullying report (2006) found that 11 per cent of UK teens had experienced cyberbullying.
- Noret and River's four-year study on bullying (2006) found that 15 per cent of the 11,227 children surveyed had received nasty or aggressive texts and e-mails, and demonstrated a year-on-year increase in the number of children who are being bullied using new technology.

- 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.

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.

A brief introduction to the technology

Mobile phones

Children 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 e-mail 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.

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/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.

- Mobile phones and bullying – Mobile phones have been used to cyberbully in a number of different ways: making nasty calls, sending nasty text messages, taking and sharing humiliating images, and videoing and sharing acts of bullying and assault via camera phone (sometimes misleadingly called 'happy slapping'). 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 Protocol (VoIP)

Instant messenger (IM) is an application that allows the user 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.

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.

Voice over Internet Protocol (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.

- Benefits – Typically children use IM 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 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 IM 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

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 may take place over several months. Some message boards are moderated – no new messages will be published publicly until the owner reviews them. However, 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 e-mail 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 the resources section on page 53 for educational and awareness materials about 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.

E-mail

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

- Benefits – As well as the obvious communication benefits, web-based e-mail 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 e-mail.
- Risks – E-mail can be used to send inappropriate images and to forward private information. Computer viruses and spam are common e-mail hazards. Web-based e-mail can also be used by people wanting to remain anonymous in order to send malicious or nasty mail.
- E-mail and bullying – People can send bullying or threatening messages by e-mail, or repeatedly send unwanted messages. Unsuitable images or video clips can be passed on. Personal e-mails can be forwarded inappropriately. The majority of computer viruses are forwarded by e-mail.

Webcams

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, for example undressing or acting in unsuitable ways. Once someone else has content the child or young person would not like their parents/carers to know about or be made public, they are at risk of being further manipulated or threatened.

Social network sites

Popular social networking websites such as Facebook and MySpace let users create their own homepages, set up weblogs and add friends. Social network sites typically allow the user to set up a profile page, listing their interests and other details, and they support contact with other users. Many focus on interests or services, e.g. 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.

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 should 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/carers 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 these can often be restricted or require approval), 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

Images and video can be posted to blogs, social networking sites and sent by e-mail. 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, e.g. 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. Firstly, children may access inappropriate material (for example, violent or pornographic content) and secondly 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 learners have been victim to content posted 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)

Many schools now use software that creates a site especially designed for education, called a virtual learning environment (VLE). Programmes such as Moodle allow school staff to set assignments, tests and activities and to track their learners' 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 learners 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 learners to access resources from home.

- Risks – If the site is accessible from any internet location, schools will want to ensure that a specific acceptable user policy is in place. Although users are tracked, learners 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, learners may still misuse the platform or post inappropriate messages or images VLEs usually consist of a range of tools, e.g. 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

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 send messages to one another. Virtual worlds – such as 2-D or 3-D online sites (for example Teen Second Life) 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 (for example, dance mats) can provide children and young people with a fun way to exercise. There are now many ways of using game software within education, for example Wordshark which is a collection of games designed to support learners with dyslexia. Virtual worlds can be used to explore and bring to life a range of topics, for example the recreation of ancient cities and NASA's Space Flight Museum in Second Life.
- 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/carers 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.

Section 2: The law relating to cyberbullying

Strong legislation exists (for Wales, for the whole of the UK and internationally) which aims to protect the rights of children and young people to a life free from abuse and harm, including bullying. Existing legislation, with relevance for bullying in general, includes:

- Education and Inspections Act 2006
- Children Act 2004
- Education Act 2002
- The Government of Wales Act 1998
- Human Rights Act 1998
- United Nations Convention on the Rights of the Child (UNCRC)
- Equality Act 2010.

Education law

Schools have a legal duty to ensure cyberbullying is dealt with in schools. Under the Education and Inspections Act 2006, headteachers, with the advice and guidance of governors and the assistance of school staff, must identify and implement measures to promote good behaviour, respect for others, and self-discipline among learners, and to prevent all forms of bullying. This includes the prevention of cyberbullying.

The Education and Inspections Act 2006 outlines some legal powers which relate quite directly to cyberbullying. Headteachers have the power 'to such extent as is reasonable' to regulate the conduct of learners 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 learners involved.

The Education and Inspections Act 2006 also provides a defence for school staff in confiscating items from learners. 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. School staff may request a learner to 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 themselves search through the phone in an appropriate case where the learner is reasonably suspected of involvement. For more information, see www.wales.gov.uk/topics/educationandskills/schoolshome/pupilsupport/inclusionpupilsupportguidance/?lang=en

Civil and criminal law

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, including threatening and menacing communications. Some cyberbullying activities could be criminal offences under a range of different laws.

- **Protection from Harassment Act 1997**
  This Act is relevant for incidents that have happened repeatedly (i.e. on more than 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. A civil court may grant an injunction to restrain a person from conduct which amounts to harassment and, following conviction of an offence under Sections 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. 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.

- **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.

- **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. 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.

- 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**, in addition to civil laws on confidentiality and privacy.

- Under the **Crime and Disorder Act 1998**, an anti-social behaviour order (ASBO) 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 ten 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 a person or persons 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 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. 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 Wales and England) 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.

Section 3: Preventing cyberbullying

There are two main elements to anti-bullying work:

- preventative work – which is ongoing and sustained, providing a consistent ethos and framework for a school's actions (this is looked at in this section)
- responsive work – which comes into effect when bullying occurs, and is most effective within a consistent whole-school approach to preventative work (this is looked at in the next section).

A whole-school approach to preventing bullying – Saundersfoot Community Primary School

Underlying all policies and procedures is the concept that all are equal, precious and valued. This thinking is pivotal to the school's ethos. The school uses a number of strategies in dealing with issues of bullying, dependent upon the particular case. However, the underlying structures and protocols remain the same. The focus is always on promoting good behaviour and putting in place systems that reward and acknowledge the positive.

Our strategies include the following.

- A clear and coherent positive behaviour policy that has been devised in consultation with all stakeholders. Shared ownership of the procedures is key to success. The school also has an anti-bullying policy that sits alongside the strategies for positive behaviour. This policy is rarely needed.
- The use of circle time to raise awareness of what is meant by bullying. Learners have the opportunity to consider the unacceptable nature of bullying and to see that reporting a bully comes from a position of strength not weakness.
- A 'zero-tolerance' approach to bullying behaviour.
- Sound supervision at play and lunchtimes with Year 5 learners acting as playground buddies. The learners have painted a buddy stop and taken assembly to explain what this means and how they can support those who feel lonely.
- Year 6 learners are appointed as class prefects to younger classes. They go on class trips with their class. They provide support and an opportunity for younger learners to talk to a trusted older child.
- Constant reinforcement of the school golden rules through class and school assemblies.

- The strong commitment of the school to 'values education' and to embedding qualities such as respect, honesty and care.
- A clear rewards system where children work together to earn whole-school rewards.
- The high profile of the school's council who take assemblies, attend anti-bullying conferences and work together with other local schools. High profile is given to national Anti-bullying Week or similar campaigns.
- Raising and discussing current issues in the news with learners through circle time, assemblies and PSE lessons.
- An open-door policy with parents/carers to address any concerns as soon as they arise.
- Regular staff INSET linked to issues such as internet safety, use of mobile phones, the use of social networking sites, etc.

The importance of a whole-school approach to preventing cyberbullying

Taking a whole-school 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, are key to effectively preventing and dealing with cases.

Respecting Others: Anti-Bullying Guidance National Assembly for Wales Circular No: 23/2003 sets out general advice on developing a whole-school policy on bullying. This section focuses more specifically on preventing cyberbullying.

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/carers, school leaders, governors, and all the people who provide support – including teaching assistants, breaktime 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.

Coordinating responsibility

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. This is essential in the context of the time and other resource challenges which staff have to manage. School staff with responsibility for pastoral care, behaviour and IT systems, as well as the school council, parents/carers and teacher unions/professional associations representing staff, will need to work together.

It is useful to identify key partners from outside agencies who can support your school in tackling cyberbullying. The police, your local safeguarding board, and a member of your local authority (if they are providing you with internet services) are recommended. Sharing resources, practices and ideas with anti-bullying leads from other schools can help ensure joined-up and effective prevention planning.

A prevention framework for cyberbullying

There is no single solution to the problem of cyberbullying; it needs to be regarded as a live and ongoing issue. The rest of this section outlines a prevention framework made up of the five essential action areas. Together they offer a comprehensive and effective approach to prevention, and should be considered as part of a whole-school approach to cyberbullying. These are:

- 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.

Prevention needs to reflect the culture, needs and preferences of the individual school community. A cyberbullying strategy will need to align with existing anti-discrimination work, curriculum delivery within PSE, and the work undertaken on social and emotional competence (see Section 1 of the overview document for more information).

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.

Valley and Vale Community Arts in partnership with Ogmore Comprehensive School – *Cyberbully*: A film and drama project

Valley and Vale Community Arts had been working alongside the Pupil Support Officer of Ogmore School for some time with learners who had been identified as having problems with anger management, bullying issues or low self-esteem. They were running drama workshops for emotional health. Each series of workshops lasted six weeks with a two-hour session each week. In between visits the learners involved were able to contact Pupil Support at any point if they needed extra support. It was as a result of these sessions that some of the young people decided they wanted to make a film, and they felt that cyberbullying was a really relevant issue for them. Their drama and film workers worked with the group to devise, script and film *Cyberbully*. The story was fictional but based on their real-life experiences.

The group gained a huge amount of confidence and self-belief through every part of the process. Once the film was finished they then went on to present it to the entire school on Respecting Others Day, and from there to other schools and events around Bridgend, including an INSET event at ESIS.

A key impact *Cyberbully* had within the school was to highlight Ogmore School's peer support system which was effective in helping learners understand the processes and help available to them.

Cyberbully was sent to every comprehensive school in Bridgend and was also purchased by Rhondda Cynon Taff Healthy Schools for all comprehensive schools. The film comes with an accompanying teaching pack making it an effective PSE resource. It was also nominated for the ZOOM Cymru Film Awards.

The learners believe that this project was effective for a number of reasons.

- Valley and Vale developed an excellent relationship with Ogmore School, where communication was paramount. This was achieved by the dedication of the school's Pupil Support Officer to the project during the workshops and during the school week in between.

- Before the *Cyberbully* project started, all participants had completed a series of drama workshops aimed at tackling anger and self-esteem issues. During this process an environment of openness and trust developed.
- The workshops were run by Valley and Vale one morning a week, but in between those times all participants had a chance to check with the Pupil Support Officer about any issues that may have arisen for them as part of the process.
- The promotion of the film and the teaching pack on completion meant that the resource became accessible to many other young people across South Wales, helping teaching and youth work professionals tackle the difficult issue of cyberbullying.

Understanding and talking about cyberbullying

Cyberbullying is an issue that is already on your school's agenda. Cyberbullying prevention is an important way of working towards improved outcomes for children and young people, and of safeguarding the health and well-being of your school community.

Developing and agreeing 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.

Promoting awareness and understanding about cyberbullying

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. It is good practice if 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.

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 special educational needs (SEN) and disabilities, should be addressed within any discussion and understanding.

Sketty Primary School, Swansea

Sketty Primary School helped the children to consider how invasive cyberbullying can be. All classes had discussions about what it is, how it happens, who you should tell and how to stop it happening.

The school linked the week to the Rights Respecting Schools Project and used the event as a launch. The main point being that while the school has rights we must accept our responsibilities – we have a right to a good education but our responsibilities are to ensure no bullying goes on. All the children made a kite with 'right' and 'responsibilities' on them and flew them in the yard before taking them home. The school also did a drama club presentation.

As a result, the children know what cyberbullying is and how to deal with it.

Publicising sanctions

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

Providing information about out-of-school bullying

Under the Education and Inspections Act 2006, the school has powers in relation to out-of-school bullying. Staff members and governors will need to understand what these are, so that they can deal with or refer cases appropriately. Learners and parents/carers will need to know that the school can provide them with support if cyberbullying takes place out of school. Revised guidance for schools covering the behaviour and conduct of learners outside schools was issued by the Welsh Assembly Government in October 2010 and is available at www.wales.gov.uk/topics/educationandskills/schoolshome/pupilsupport/inclusionpupilsupportguidance/?lang=en

Updating existing policies and practices

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, e.g. staff development, ICT support and infrastructure, e-safety policies and e-learning strategies.

Reviewing and updating policies to include cyberbullying

School governors, headteachers 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.

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.

Reviewing existing acceptable use policies (AUPs)

Acceptable use policies (AUPs) outline the way in which new and emerging technologies may and may not be used by learners and staff in order that they can use the ICT facilities in school. If you only have these online, you might want to produce a paper form that can be sent home for parents/carers 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 responsibilities of use, sanctions for misuse, and issues around confiscation and retention.

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. 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/carers are aware of such measures. (Parents/carers may currently contact their child by mobile phone 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.)

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.

Making reporting cyberbullying easier

Reporting any incident of bullying can be really hard for the person being bullied and for bystanders. It is important therefore 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.

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.

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

Schools are advised to provide parents/carers with information about cyberbullying policies, procedures and activities, and opportunities for becoming involved in these. This could be done in several ways including:

- through an assembly or event which parents/carers are invited to attend
- through letters home
- by posting information on the school website.

Children, young people and parents/carers will need information about all the ways they can report concerns and incidents and what they should expect to happen in return.

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.

Exploring different reporting routes

There are a range of strategies, including learner-centred strategies, which schools successfully adopt to both raise awareness of bullying issues and offer learners alternative reporting routes. This full range should be applied to cyberbullying.

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

Setting up a cyberbullying taskforce, made up of learners 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 council or an existing bullying or healthy schools group.

Involving 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.

Signposting information about external reporting routes

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 and schools can provide this information by letter to parents/carers or from an area on their own websites.

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 signpost clearly 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.

Promoting the positive use of technology

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.

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.

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.

Reviewing existing staff development targets and opportunities

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.

Schools might review existing staff development targets and opportunities, and look at including e-safety issues as an important component of technology for education. Schools should look at training and support opportunities for school leaders and governors, as well as teachers, support staff and extended schools provision staff.

Promoting e-safety and digital literacy

Exploring safe ways of using technology with learners may help 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. 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.

Ensure that all staff and learners 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 learners and staff members never leave logged-in accounts unattended.

Protecting passwords

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 might include a parent/carer or the police) and never let anyone use their accounts.

The school's acceptable use policy (AUP) – the agreement between learners and the school which outlines the responsibilities of learners using the school's computer network and equipment – may usefully refer to password privacy. It should also be covered in any internet safety lessons or induction to school accounts that might be password protected (for example, the VLE).

Reviewing how the school network is monitored

The ability to conduct searches of internet-use records at school is an important part of being able to investigate incidents of cyberbullying. Your school may want to review and investigate available software, for example, monitoring software and key logging programmes. It is important that learners and staff 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.

Evaluating the impact of prevention activities

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.

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 also important to communicate to parents/carers and the whole-school community why this happens in the short term, and to recognise that reducing incidents is a longer-term goal.

Conducting a regular survey

Schools could conduct an annual survey of learners' experiences of bullying. Cyberbullying incidents could be included in such a survey. This will provide schools with a good overview of how common cyberbullying incidents are among learners, 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.

Many schools already use learner and staff satisfaction surveys. It is useful also to conduct a parent/carer satisfaction survey. Asking questions about cyberbullying will provide you with an indication about awareness and the success of your prevention work.

Publicising progress and activities to the whole-school community

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

Section 4: Responding to cyberbullying

Preventative work should aim to minimise the occurrence of bullying. However, even where effective preventative work is undertaken, some incidents will still occur. This is where responsive work should come into effect, but it is most effective within a consistent whole-school approach to preventative work, as looked at later in this section.

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

Cyberbullying is a form of bullying

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.

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/carers should be informed as appropriate, and those found to be bullying should be interviewed and receive appropriate sanctions.

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 is 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 any-place nature of cyberbullying
- anonymity – the person being bullied will not always know who is attacking them
- motivation – some learners 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 on page 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.

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

- supporting the person being cyberbullied
- recording and investigating cyberbullying incidents
- working with those who cyberbully and applying sanctions.

These will each be looked at in the subsections that follow.

Supporting the person being cyberbullied

As with other forms of bullying, the target of cyberbullying may be in need of emotional support. Key principles here include:

- encouraging learners to seek help
- reassuring them that they have done the right thing by telling someone
- recognising that it must have been difficult for them to deal with
- reiterating that no one has a right to do that to them
- taking steps to ensure the school adopts a culture that does not tolerate cyberbullying, as this can also help to make the target of cyberbullying feel safe.

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.

Advice on online empowerment

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/carer or a member of staff.

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

Advising a child to change their contact details, such as their instant messenger (IM) 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

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, for example embarrassing images, has been circulated, it is important to look at whether this content can be removed from the web.

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.
- 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' on page 46). 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 learners 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 (Section 94). However, staff do not have a right to search through learners' mobile phones unless the school's behaviour policy expressly provides for this and the learner is reasonably suspected of involvement in an incident of cyberbullying which is of a sufficiently serious nature.

- 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.

> Thankfully my son's school were very helpful. They identified the child who posted the video from another video he had posted, and 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.

(Parent)

As previously stated, members of the school workforce, as well as learners, 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 in the previous bullet points to ensure the well-being of staff.

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

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 e-mail or instant messenger buddy list will mean that they will not receive messages from that particular sender anymore.

Learners or their parents/carers 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. The 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

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. Details of how to contact the phone operators can be found in Section 5.

Social networking sites

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. 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. It is good practice for social network providers to make reporting incidents of cyberbullying easy, and thus have clear, accessible and prominent reporting features. 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 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. Children and young people may also choose to 'Click CEOP' to report issues with a website.

Instant Messenger (IM)

It is possible to block users, 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 IM 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. It is also good practice for IM providers to have visible and easy-to-access reporting features on their service.

E-mail providers (e.g. Hotmail and Gmail)

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

Video-hosting sites

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. YouTube provides information on what is considered inappropriate in its terms of service, see www.youtube.com/t/terms Children and young people may also choose to 'Click CEOP' to report issues with a video-hosting site.

Chatrooms, individual website owners/forums, message board hosts

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 prominent reporting mechanism to enable the user to contact the service provider. Users that abuse the service can have their account deleted. Children and young people may also choose to 'Click CEOP' to report issues.

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 player's name and conduct to the game site administrator.

Recording and investigating cyberbullying incidents

Preserve the evidence

Schools should advise learners and staff to try to keep a record of the incident, recording:

- the date and time
- the content of the message(s)
- where possible a sender's ID (e.g. username, e-mail, mobile phone number) or the web address of the profile/content
- an accurate copy or recording of the whole web-page address.

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/carers, teachers, pastoral care staff and the police.

How to do this

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, in some cases, forwarding messages, for example to a staff member's phone, can 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. 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 the 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 e-mail, 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).

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 the local police if illegal images have been taken of a child and circulated. Similarly if there is a recording of a crime, for example assault on another child, contact the local police.

Where internet content may contain child sexual abuse content, criminally obscene adult content and incitement to racial hatred, contact Internet Watch Foundation at www.iwf.org.uk or 'Click CEOP'.

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' on page 44).

Identifying the bully

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 e-mail account to send nasty messages.

In cases where you do not know the identity of the bully, some key questions to consider include the following.

- 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)? 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.
- 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 learner may be able to identify the number or the school may already keep records of the mobile phone numbers of their learners. Content shared through a local wireless connection on mobile phones does not pass through the service providers' network, and is much harder to trace. Similarly text messages sent from a website to a phone also provide difficulties for tracing 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 and any evidence of sexual exploitation (e.g. grooming or inappropriate sexual contact or behaviour).

Working with those who cyberbully and applying sanctions

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.

Steps should be taken to change the attitude and behaviour of those who cyberbully, as well as to ensure access to any support that they may need. It is important to ensure that the person using cyberbullying 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.

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 person using cyberbullying to disguise their identity
- the public nature of posted material (and the extent of the humiliation)
- the difficulty in controlling copies of the material (the difficulty in gaining closure over the event).

It should also be recognised that where induction and education activities are not in place 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 person carrying out cyberbullying. Consideration should also be given to the possibility that the cyberbullying could be a part of retaliation to previous bullying endured by the perpetrator.

Sanctions for bullying behaviour

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 detering 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.

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.

Technology-specific sanctions for learners 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).

Section 5: Resources and further reading

The Welsh Government does not necessarily endorse all the views expressed by these publications, websites and organisations.

Publications

ATL: Cyberbullying

This factsheet explains the problem of cyberbullying, what steps teachers should take if they are a victim of cyberbullying, and what schools should be doing to tackle the problem.
www.atl.org.uk/publications-and-resources/factsheets/cyberbullying.asp

A teacher's guide to using Facebook

Written by Bernadette Rego, this American guide concentrates on how teachers can benefit from Facebook and avoid potential pitfalls.
www.anti-bullyingalliance.org.uk/pdf/facebook_guide_teachers.pdf

Cyberbullying – A whole-school community issue (2007)

A short booklet from Childnet International.
www.childnet-int.org/downloads/cyberbullyingOverview.pdf

Incoming Message

'Incoming Message' is a 10-minute film which follows the story of a case of text bullying, and the consequences for all those involved. It is available free to secondary schools from Orange.
www1.orange.co.uk/about/corporateresponsibility/quicklinks/educational_resources/text_bullying.html

Know IT All

Know IT All (KIA) is Childnet's award-winning suite of free education resources designed to help educate parents/carers, teachers and young people about safe and positive use of the internet. Currently there are four KIA resources for parents/carers, secondary schools, primary schools and trainee teachers and all four resources include content for young people.
www.childnet-int.org/kia

Let's fight it together

Produced by Childnet International, this film addresses the issue of cyberbullying. As well as the drama illustrating cyberbullying, there are interviews with the main characters, a drama documentary produced by Year 11 learners with an accompanying lesson plan, teaching notes, and an interactive resource highlighting key issues. For a copy of the DVD, please e-mail PETshare@wales.gsi.gov.uk
www.digizen.org/cyberbullying/film.aspx

The Byron Review (2008) – Safer Children in a Digital World

An independent review looking at the risks to children from exposure to potentially harmful or inappropriate material on the internet and in video games. A summary for children and young people is also available. This has been followed by a review of progress called *Do we have safer children in a digital world? – The Byron Progress Review (2010)*. This review contains a section on improving education in terms of internet activity and safety. All documents can be accessed from www.education.gov.uk

Useful websites

Websites for children and young people

Anti-Bullying Alliance

The ABA brings together over 130 organisations into one network with the aim of reducing bullying and creating safer environments in which children and young people can live, grow, play and learn. The ABA produce resources and tools to help schools and local authorities develop anti-bullying strategies. The ABA national coordination team is based at National Children's Bureau.
Tel: 020 7843 1901
e-mail: aba@ncb.org.uk
www.anti-bullyingalliance.org.uk

Bullying UK

Cyberbullying advice sub-site of Bullying UK. Access to the site is also available on mobile phones.
www.cyberbullying.co.uk

Chatdanger

A website about the potential dangers online (including bullying), and advice on how to stay safe while chatting.
www.chatdanger.com

Child Exploitation and Online Protection Centre (CEOP)

Set up in 2006, they deal with child sexual exploitation, and it is possible to report directly to them online. 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.
www.ceop.gov.uk

Childnet International

A range of resources for primary and secondary schools, children and young people, teachers and parents/carers.
www.childnet-int.org

CLIConline
The Welsh Government's national information and advice service for young people aged 11 to 25, provides information on bullying.
www.cliconline.co.uk

Cyberbullying.org
One of the first websites set up in this area for young people, providing advice around preventing and taking action against cyberbullying. It is a Canadian-based site.
www.cyberbullying.org

CyberMentors
This site is all about young people helping and supporting each other online.
www.cybermentors.org.uk

Internet Safety Zone
Useful information for parents/carers, teachers and children on cyberbullying and how to tackle it.
www.internetsafetyzone.co.uk

Internet Watch Foundation
They can be contacted where internet material may contain child sexual abuse content, criminally obscene adult content and incitement to racial hatred.
www.iwf.org.uk

Kidsmart
This site contains a range of resources and activities for children, young people and parents/carers, including lesson ideas for teachers. Produced by Childnet International.
www.kidsmart.org.uk

London Grid for Learning (LGfL)
The LGfL website has a number of resources in its e-safety section, including hints and tips for teachers about social networking sites and a model acceptable use policy.
www.lgfl.info

Meic
Meic is the Welsh Government-funded bilingual national advocacy service for children and young people in Wales.
www.meiccymru.org

StopText bully
A website dedicated to mobile phone bullying, which contains advice for young people including how to contact your operator.
www.stoptextbully.com

Teachtoday

Teachtoday is a website that provides information and advice for teachers, headteachers, governors and other members of the school workforce about the positive, responsible and safe use of new technologies.
www.teachtoday.eu

Thinkuknow (TUK) – teachers and trainers area

Here you'll find resources for teachers and all other professionals working with young people. There are films, presentations, games, lesson plans and posters covering a range of issues from grooming by child sex offenders to cyberbullying. All of these resources encourage young people to have fun with new technology, while staying in control of the risks. Importantly, they also teach young people where to go if they have any concerns.
www.thinkuknow.co.uk

UK code of practice for the self-regulation of new forms of content on mobiles (2004)

This code outlines the mobile operators' commitment to deal vigorously with malicious communications.
www.imcb.org.uk

UK Council for Child Internet Safety (UKCCIS)

Brings together over 150 stakeholders from across the internet safety spectrum to work on internet safety. UKCCIS launched the 'Click Clever Click Safe' campaign to promote internet safety among children and parents/carers.
www.education.gov.uk/ukccis

Wise Kids

A site promoting innovative, positive and safe internet use. It has advice and resources for educators, as well as young people, parents/carers, communities and business.
www.wisekids.org.uk

Details of how to contact mobile phone operators

- **O2:** Call 08705 214000 or e-mail ncb@O2.com
- **Vodafone:** Call customer services on 191 from a Vodafone phone or on any other phone call 08700 700191 for Pay Monthly customers or on 08700 776655 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 e-mail using the 'How to contact us' section of the T-Mobile website at www.t-mobile.co.uk

Advice for parents/carers and children and young people on cyberbullying

In working to prevent and respond to cyberbullying, schools should work with parents/carers and the children and young people themselves. The short sections that follow are aimed at parents/carers and children and young people, and could be used by schools as part of their work.

Advice for parents/carers on cyberbullying

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 way in which they are using the internet and their mobile phone. In 'Advice for children and young people on cyberbullying' (page 59) there is an anti-cyberbullying code which contains seven key messages for children. You may find this 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.

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.

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 (shown on page 59). These include 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 e-mails, 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 learner or learners 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 sanction the learner 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. Facebook or Bebo). 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. Many website and social networking sites contain a 'Click CEOP' button. CEOP is a national agency called the Child Exploitation and Online Protection Centre and aims to deal with child sexual exploitation and safety online (www.ceop.gov.uk).
  - 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).

Advice for children and young people on cyberbullying

Being sent an abusive or threatening text message, or seeing nasty comments about you on a website can be really upsetting. The seven points here are an 'anti-cyberbullying code' which gives you important tips to protect yourself and your friends from getting caught up in cyberbullying, and advice on to how to report it when it happens.

- **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.
- **Think before you send** – It is important to think before you send any images or text about yourself or someone else by e-mail 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?
- **Treat your password like your toothbrush** – Don't share your passwords with anyone else. 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, only give your mobile number or personal website address to trusted friends.
- **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!
- **Don't retaliate or reply** – Replying to bullying messages, particularly in anger, is just what the bully wants.
- **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.

- **Make sure you tell someone** – You have a right not to be harassed and bullied online. There are people who 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 your school. Your teacher or the anti-bullying coordinator at your school can support you and can discipline the person bullying you.
  - 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.
  - On many websites you can choose to use the 'Click CEOP' button if you are concerned about something that has happened online. They are a national organisation giving help and advice on areas such as cyberbullying, hacking, viruses and mobile problems. They also have the option to report any instance of sexual behaviour or harmful content.
  - 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?

What children and young people say

The comments on the following pages come from a Childnet survey of primary- and secondary-aged learners. These views are included to give a young person's perspective on the issue of cyberbullying.

Many of the learners had experienced cyberbullying personally, or had friends who had been cyberbullied. The vast majority of the learners 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/carers, and many reported helping teachers or parents/carers with mobile phones and websites.

Reasons given why learners 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 who 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/carers, and their headteacher.
- In some cases they felt safer contacting expert groups – they talked about phoning ChildLine and also e-mailing 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.

Acknowledgements

The Welsh Government would like to thank those who provided case studies and information for this document, as well as others in the anti-bullying guidance series.

- Cardiff Council working in partnership primarily with Safer Wales, LGBT Excellence Centre and Cardiff Against Bullying
- Cathays High School, Cardiff
- Duffryn High School, Newport
- Gorseinon Infant School, Swansea
- Hafod y Wern Primary School, Wrexham
- Markham Primary School, Caerphilly
- Ogmore Comprehensive School, Bridgend
- Pembroke Comprehensive School, Pembrokeshire
- Saundersfoot Community Primary School, Pembrokeshire
- Sketty Primary School, Swansea
- St Richard Gwyn Catholic High School, Flintshire
- St Teilo's Church in Wales School, Cardiff
- Terrence Higgins Trust
- Torfaen County Borough Council
- Valley and Vale Community Arts
- Youth Offending Service (Restorative Justice in Schools Coordinator), Bridgend
- Ysgol Gymraeg Bro Ogwr, Carmarthenshire