Conclusion

Cyberbullying can be very damaging to individuals, and disruptive to school life. School staff have been targeted as well as pupils, and cyberbullying can adversely effect their well-being and the important contribution that they make to their school community. Though new technology brings incredible opportunities for educators as well as young people, it is crucial that everyone knows how to use this technology responsibly and that policies are in place to support and encourage responsible use. School staff should be aware of what cyberbullying is, and be clear about how they report it and the support in place to help them deal with incidents quickly and effectively. School leaders should ensure that measures are in place to identify, prevent and respond to cyberbullying, based on the Government's **Safe to Learn: Cyberbullying** guidance. They should ensure that their work in this area includes and supports school staff, and that they have policies and practices in place to meet the specific needs of school employees.

"Every individual has a right to be respected at their place of employment and bullying of any kind is a violation of that right, so I hope that this guidance is used by all staff members and schools to prevent cyberbullying of staff and reduce the harm and hurt it can cause."

"Bullying of any kind is harmful and, as it evolves alongside technological advances we see new forms, such as cyberbullying, making their mark. I know children are not the only victims of this humiliating form of bullying, school staff are too. That is why this guidance has been produced specifically to help and support school staff tackle cyberbullying. It provides straightforward advice and will help school staff know their rights and the powers they and schools have to deal with cyberbullying."

Rt Hon Ed Balls MP
Secretary of State for Children, Schools and Families

"The potential benefits of the internet, mobile phones and new technologies are enormous for all of us – adults as well as children and young people. Increasingly, the use of and confidence with technology is critical for our work, social and civic lives. Bullying in any form should never be acceptable, and we know from talking to school staff and hearing their stories that cyberbullying can cause real pain to those on the receiving end. We hope that this guidance will provide the practical information and advice that schools and individual employees need to ensure that their whole-school communities are equipped to prevent and respond to cyberbullying."

Will Gardner
CEO, Childnet International
www.childnet.com

To find this Guidance online together with resources for schools in tackling cyberbullying see:

www.digizen.org

ARE YOU A RESPONSIBLE DIGITAL CITIZEN?
PLAY THE NEW digizen interactive

digizen.org

LGE
Local Government Employers

This Guidance is supported by the Local Government Employers

You can download this publication or order copies online at **www.teachernet.gov.uk/publications**. Search using the ref: DCSF-00242-2009. Copies of this publication can also be obtained from: **DCSF Publications, PO BOX 5050, Sherwood Park, Annesley, Nottingham NG15 0DJ**. Tel: 0845 60 555 60; fax 0845 60 333 60; textphone: 0845 60 555 60. Please quote ref: 00242-2009BKT-EN; ISBN number: 978-1-84775-362-5.

This document has been printed on 80% recycled paper

department for
children, schools and families

Cyberbullying

Supporting School Staff

Introduction

Staff in schools, as well as children and young people, may become targets of cyberbullying. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. It may have a significant impact not only on the person being bullied, but on their home and work life too. Career progression may be affected, and there have been cases where the person bullied has chosen to leave the education sector altogether. Dealing with incidents quickly and effectively is key to minimising harm in potentially highly stressful situations.

All employers including employers of school staff have various statutory and common law duties to look after the physical and mental health of their employees. Protecting staff from cyberbullying is best done within a prevention framework, with whole school policies and practices designed to combat cyberbullying. Each school should have a designated cyberbullying lead, a member of the senior management team tasked with overseeing and managing the recording, investigation and resolution of all bullying incidents.

The Department for Children Schools and Families (DCSF) has produced comprehensive advice on cyberbullying as part of the Safe To Learn guidance, which can be accessed online along with support materials from **www.digizen.org/cyberbullying**.

Safe To Learn: Cyberbullying was made available and promoted to UK schools in 2008, and provides a robust framework to enable the effective prevention of, and response to, cyberbullying incidents. Every school should review relevant behavioural policies and procedures, in order to take account of current DCSF advice on cyberbullying.

Cyberbullying: Supporting School Staff has been written by Childnet International for the Department for Children, Schools and Families, in consultation with the DCSF Cyberbullying Taskforce, and with the support of the leading school employee unions and professional associations. This document builds on the **Safe To Learn** guidance, and provides information for employers of school staff – Local Authorities and governing bodies. It also offers advice for school staff about keeping themselves and their personal information safe.

Childnet International

What is Cyberbullying?

Cyberbullying is the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else.

Information and Communication Technologies are key within education to support learning and school systems but they can also be misused.

Cyberbullying may consist of threats, harassment, embarrassment, humiliation, defamation or impersonation. Cyberbullying may take the form of general insults, or prejudice-based bullying, for example homophobic, sexist, racist or other forms of discrimination.

There have been cases of school employees being cyberbullied by current or ex-pupils; by colleagues, parents and other adults; and by people who attempt to remain anonymous.

There are reported cases of cyberbullying involving email, Virtual Learning Environments, chat rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

Some features of cyberbullying are different to other forms of bullying:

- Cyberbullying can take place 24/7. Incidents can take place in the victim's own home, intruding into spaces that have previously been regarded as safe and private.
- The audience can be very large and reached rapidly. The difficulty in controlling electronically circulated messages means the scale and scope of cyberbullying can be greater than for other forms of bullying. Electronically-forwarded content is hard to control, and the worry of content resurfacing can make it difficult for the person being bullied to move on.
- The profile of the person being bullied and bully may not rely on traditional power imbalances – a cyberbully may not be older, or physically stronger, or hold a position of greater authority than their victim.
- Unlike other forms of bullying, the target of the bullying will have evidence of its occurrence. The bully will leave a 'digital footprint' that can potentially be used as evidence against them.
- In some cases, incidents of cyberbullying may be unintentional. The person responsible may not realise that remarks are publicly accessible and persistent, or understand the amplified effect that technologies produce. They may not be fully aware of the potential seriousness or impact of their actions. Therefore prevention activities are key to ensuring the whole-school community clearly understands the serious consequences of cyberbullying, including sanctions.

> "The Police were called to a school to resolve allegations made against a male teacher. The teacher was apparently using Instant Messenger to contact female members of his class encouraging them to expose themselves on webcam. After investigation, it turned out to be 2 boys in his class, because 'they didn't like him.'"

The scale of cyberbullying against school staff

Current research into the frequency of and impact on school employees of cyberbullying is not extensive. We do know that cyberbullying incidents can be extremely upsetting – even devastating – for the person being bullied, whatever age they are.

Cyberbullying of school staff is an issue that schools need to address within their whole-school cyberbullying strategy.

- 15% of teachers responding to a 2009 survey carried out by Teacher Support Network and The Association of Teachers and Lecturers reported they had been victims of cyberbullying.
  http://icanhaz.com/teachersupport
- 46% of teachers surveyed for Becta's E-Safety and Web 2.0 Report (September 2008) reported negative experiences caused by pupils using web 2.0 technologies (defined as participatory mobile and web-based sites and services).
  http://icanhaz.com/BECTAsurvey
- In May 2007 the NASUWT surveyed teachers over a period of 5 days on cyberbullying. Almost 100 teachers reported incidents of cyberbullying by pupils using mobile phones and web-based sites that had caused real distress and trauma.
  www.nasuwt.org.uk/cyberbullying

School workforce unions, professional associations and industry providers have noted an increase in cyberbullying reports and related inquiries, and are committed to working with the DCSF to reduce incidence and support schools to deal with incidents effectively.

All forms of bullying, including cyberbullying, should be taken seriously. Bullying is never acceptable, and should never be tolerated.

Cyberbullying and the law

While there is not a specific criminal offence called cyberbullying, activities can be criminal offences under a range of different laws, including:

- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988,
- Section 127 of the Communications Act 2003
- Public Order Act 1986
- The Defamation Acts of 1952 and 1996

Cyberbullying in the form of discrimination or harassment of a member of staff by another member of staff may result in a situation where the governing body of a school has breached its duties under discrimination legislation.

It is the duty of every employer to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees.

Incidents that are related to employment, even those taking place outside of the hours or place of work, may fall under the responsibility of the employer.

> "Pupils set up a web page with photographs taken on a mobile phone in school, obviously without me knowing. The site included threatening comments and offensive language. I printed the pages of the site to keep a hard copy and this was used to investigate who was responsible. The Principal interviewed all the pupils involved with their parents and has excluded the main author of the site until her exams in May. Others had fixed-term exclusions ranging from 2 to 5 days depending on the severity of their comment."
> **A staff member**

Whole-school community steps to effectively tackle cyberbullying

Every school should have robust policies in place that include the acceptable use of technologies by pupils and staff and address cyberbullying. Agreements on the responsible use of technologies need to include:

- Rules on the use of equipment, software and network access provided by the school – for example, laptops, Virtual Learning Environments, and internet access.
- The use of staff and pupil owned equipment and internet access routes, where they are used on school premises and within school hours, for example, mobile phones, digital cameras, and laptops.
- Acceptable behaviour for learners and employees including behaviour outside of school – for example teachers' and pupils' use of social networking services and other sites, insofar as harming others and bringing the school into disrepute are concerned.

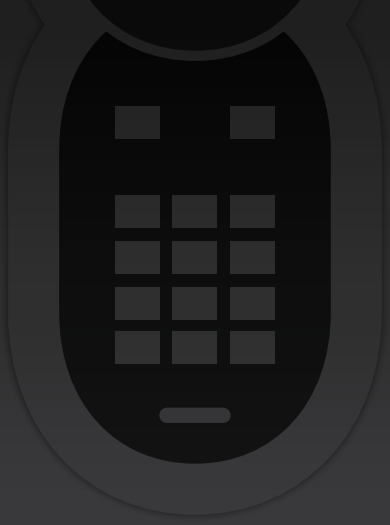
Cyberbullying issues may be addressed in contracts of employment, employee guidance and/or employee-specific acceptable use policies. Employee-specific guidelines that encompass the appropriate use of technologies should be developed in consultation with staff members, and recognised employee union and association representatives.

Whole-school policies and practices designed to combat cyberbullying should similarly be developed by and for the whole-school community. Schools will need to develop clear guidance to help to protect every member of the school community and to ensure that sanctions are appropriate and consistent. This will need to be effectively communicated to and discussed with employees, pupils and parents.

Becta provide information to support schools on developing and evaluating their Acceptable Use Policies: **http://icanhaz.com/BECTAaup**.

There is no single solution to the problem of cyberbullying; it needs to be regarded as a live and ongoing issue. An effective approach requires clearly defined responsibilities, reporting lines and co-ordination. A member of the senior management team will need to be designated as lead – preferably the member of staff who takes overall responsibility for all bullying cases.

The DCSF's Cyberbullying Guidance available from **www.digizen.org/cyberbullying** outlines a prevention framework of five key action areas that together offer a comprehensive and effective approach to prevention:



Understanding and talking about cyberbullying

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

ICT, Citizenship, SEAL and PSHE are particularly effective subjects for addressing cyberbullying with pupils, but cyberbullying education can be embedded across the curriculum, addressed in tutorials, assemblies, and parents evenings.

Updating existing policies and practices

A whole-school approach is recommended to develop new policy and practice effectively, ensuring that everyone is engaged in and aware of the schools approach to cyberbullying. School governors with the head teacher and leadership team should audit existing policies (especially behaviour and ICT policies) and procedures to decide which need to be changed or adapted in order to include cyberbullying prevention and how to respond to incidents.

Keeping good records of all cyberbullying incidents is essential to monitoring the effectiveness of your school's prevention activities, and to review and ensure the consistency of investigations, support and sanctions.

Making reporting cyberbullying easier

All staff, as well as pupils and parents, should understand the importance of promptly reporting incidents that happen to them or that they witness. The school should publicise existing reporting routes and investigate alternative routes. Pupils, staff and parents should be clear on how and who they should report to. Lines of responsibility should be clear and well understood. Staff and pupils alike should feel confident that all cyberbullying incidents will be taken seriously and effectively addressed.

Staff should also be aware of alternative routes they can access for additional support. These could include their union or professional association, the Teacher Support Network, occupational health services, Local Authority HR services, or helplines such as the Samaritans.

Promoting the positive use of technology

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.

It is increasingly important that educational employees understand how collaborative and participatory technologies, such as social networking services, are used. Comprehensive e-safety education will include support for both pupils and staff on managing personal information in online environments, and in using personal and social technologies responsibly.

Evaluating impact of prevention activities and of response actions

The school should consider how it might most effectively measure the impact of prevention activities. Pupil, staff and parent satisfaction surveys may provide an important indication of progress. Similarly, if cyberbullying activities against staff are identified, schools should review the effectiveness of actions taken against criteria such as:

- staff satisfaction with process and support
- effectiveness of sanction against the pupil
- effectiveness of sanctions in reinforcing school policy to other pupils.

Checklist

Dealing with cyberbullying is best done within a robust framework of policy and practice, which includes and supports the whole-school community. Every school should ensure that:

- School governors, head teachers, and senior management team members are familiar with the Government's **Safe To Learn Cyberbullying** Guidance. This can be found online at **www.digizen.org/cyberbullying** and at **www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying**.
- The whole-school community should understand what is meant by 'cyberbullying', it's potential impact, how it differs from other forms of bullying and why it is unacceptable.
- All staff should be provided with information and professional development opportunities regarding understanding, preventing and responding to cyberbullying. It is particularly important that they understand child protection and other legal issues that may relate to cyberbullying incidents.
- Current school policy, guidance and information relevant to cyberbullying should be reviewed, to ensure that it meets the needs of pupils and staff. These are likely to include: Behavioural agreements; Acceptable Use Policies, including the use of mobile phones and cameras within school; Employee terms and conditions; Pupil and staff support and pastoral care.
- The whole-school community should understand reporting routes and responsibilities. A member of the senior management team should be appointed to lead on and oversee anti-cyberbullying activity and incidents. Staff may find it difficult to report instances of cyberbullying to their line manager, and they should feel free to seek advice from appropriate agencies outside of the school – their union or professional association, for example, or the Teacher Support Network.
- The positive use of technology, which models safe and effective practice, is key to preventing the misuse of technology. Schools should ensure that learning strategies and targets, as well as staff development programmes, support the innovative and engaging use of technologies.
- The impact of prevention and response policies and practice should be monitored annually. Staff and pupils and parents should feel confident that their school effectively supports those who are cyberbullied.

School employees should expect:

- All incidents that they report are recorded.
- The school will respond to an incident in a timely and appropriate manner, where possible, or support the member of staff concerned to do so.
- Appropriate personal support, or information enabling them to access appropriate personal support will be provided.
- Information on the safe use of technology will be provided to them.
- The school will approach third party agencies on their behalf in order to request that inappropriate material is removed, where possible.
- The school will support the staff member in cases where it is necessary for the person being bullied to contact the service provider directly, for example where identity theft or impersonation has taken place, where an individual has a complaint about their appearance in a video, or where the incident involves contacting the staff member's mobile phone service provider.
- Where appropriate, the school will contact the police or their Local Authority Designated Officer (LADO).

Where the bully is a member of the school community:

- The school will work with and take steps to change the attitude and behaviour of the bully.
- The school will take care to make an informed evaluation of the severity of the incident, taking into account the ways in which cyberbullying differs from other forms of bullying.
- The school will deliver appropriate and consistent sanctions.

School employees should take steps to protect themselves and their personal information by:

- Keeping passwords secret and protecting access to their accounts.
- Not friending pupils on personal social networking services.
- Keeping personal phone numbers private and not using their own mobile phones to contact pupils or parents.
- Keeping a record of their phones unique International Mobile Equipment Identity (IMEI) number, and keeping phones secure while on school premises.
- Not posting information about themselves publicly that they wouldn't want employers, colleagues, pupils or parents to see.
- Ensuring that rules regarding the use of technologies are consistently enforced.
- Not personally retaliating to any incident.
- Reporting any incident to the appropriate member of staff in a timely manner.
- Keeping any evidence of an incident.

Getting offensive content taken down

Where online content is upsetting and inappropriate, and the person or people responsible for posting is known, the quickest way to get material taken down is likely to be to ensure that the person who posted it understands why the material is unacceptable and to request that they remove it.

If the person responsible has not been identified, or will not take material down, the school leadership team member will need to contact the host (for example, the social networking site) to make a report to get the content taken down. The material posted may breach the service provider's terms and conditions of use and can then be removed.

In cases where the victim's personal identity has been compromised – for example, where a site or an online identity alleging to belong to the victim is being used, the victim will need to establish their identity and lodge a complaint directly with the service provider. Some services will not accept complaints lodged by a third party. In cases of a mobile phone abuse, for example, where the person being bullied is receiving malicious calls or messages, the account holder will need to contact their provider directly.

Before a school or individual contacts a service provider, it's important to be clear about where the content is – for example by taking a screen capture of the material that includes the URL or web address. If you are requesting they take down material that is not illegal, be clear how it contravenes the site's terms and conditions.

In cases of actual/suspected illegal content, the schools designated representative should contact the police. The police will be able to determine what content is needed for evidential purposes.

Service Providers

Mobile phones

All UK mobile phone operators have nuisance call centres set up and/or procedures in place to deal with such instances. They may be able to change the number of the person being bullied. Mobile operators cannot bar a particular number from contacting a phone, but some phone handsets do have this capacity. Action can be taken against the bully's phone account (e.g. blocking their account) only with police involvement.

Contacts:

O2: **ncb@o2.com** or 08705214000.

Vodafone: 191 from a Vodafone phone or 08700700191 for Pay Monthly customers and 08700776655 for Pay as you Go.

3: Call 333 from a 3 phone or 08707330333.

Orange: Call 450 on an Orange phone or 07973100450 for Pay as you Go, or 150 or 07973100150 for Pay Monthly.

T-Mobile: Call 150 on a T-Mobile phone or 08454125000.

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

Contacts of some social network providers:

Bebo: Reports can be made by clicking on a 'Report Abuse' link located below the user's profile photo (top left-hand corner of screen) on every Bebo profile page. Bebo users can also report specific media content (i.e. photos, videos, widgets) to the Bebo customer services team by clicking on a 'Report Abuse' link located below the content they wish to report.
www.bebo.com/Safety.jsp.

Facebook: Reports can be made by clicking on the 'Report' link located on pages throughout the site, or by email to **abuse@facebook.com**.
www.facebook.com/safety.

MySpace: Reports can be made by clicking on the 'Contact MySpace' link at the bottom of every MySpace page and selecting the 'Report Abuse' option. Alternatively, click on the 'Report Abuse' link located at the bottom of each user profile page and other user generated pages. Inappropriate images can be reported by clicking on the image and selecting the 'Report this Image' option. Additionally, school staff may email MySpace directly at **schoolcare@myspace.com**.
www.myspace.com/safety.

Video and photo hosting sites

YouTube: Logged in YouTube members can report inappropriate content by using the 'flag content as inappropriate' function which appears under every video.
http://icanhaz.com/YouTubeAbuseSafety.

Flickr: Reports can be made via the 'Report Abuse' link which appears at the bottom of each page. Logged in members can use the 'flag this photo' link to report individual pictures.
www.flickr.com/guidelines.gne.

Instant Messenger

It is good practice for Instant Messenger (IM) providers to have visible and easy-to-access reporting features on their service. Instant Messenger providers 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.

Contacts of some IM providers:

MSN: When in Windows Live Messenger, clicking the 'Help' tab will bring up a range of options, including 'Report Abuse'.

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

Chatrooms, individual website owners / forums, message board hosts

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. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use.

Images and Video

Taking pictures and creating short films is easier than ever before. Employees and learners can use mobile phones, digital cameras, camcorders and webcams to capture, edit and share images. Photo and video sharing websites are extremely popular, and can be used effectively for school projects and presentations. It's important that employees and pupils are clear about their rights and responsibilities regarding taking pictures and making films.

- Photos taken for official school use may be covered by the Data Protection Act and pupils and parents should be advised why they are being taken. Schools should consider e-safety issues when using pictures of pupils.
- Photos taken for personal use are exempt from the Data Protection Act.

It is important to seek permission before sharing or posting a picture of someone publicly online. If a picture causes distress, the subject should ask the poster to remove it in the first instance and if this does not result in the image being taken down, a request can be made to the service provider to remove the picture or film that was taken and/or posted without consent.

Consent and rights management are important topics to address with the whole-school community. The acceptable use of equipment for creating images and film (which may most typically be camera-equipped mobile phones) should be accounted for within the appropriate behaviour policy and agreements. Schools should clearly communicate expectations, acceptable conduct and potential sanctions regarding inappropriate image taking and use by staff, pupils and parents.

Both pupils and employees should take care not to attach any significant personal information to publicly posted information, for example full names, without informed and/or parental consent. Even with consent, care should be taken to be mindful of basic e-safety practice.

Mobile phones

Mobile phones are increasingly sophisticated, and are typically designed to do more than make calls and send text messages. Many models can be used as music players, to store documents, to take photographs and short films. Mobiles can be used as calendars and alarm clocks, and to access the internet – in order to view, download or upload content. Using Bluetooth or infrared on equipped phones allows people to pass pictures and content between mobiles and computers without incurring any charges.

Mobiles can be used very effectively to support learning, allowing learners to document project work, for example by using images, voice and text. However, most schools have also experienced problems with the disruptive use of mobiles and should have clear guidelines about acceptable use, developed in consultation with the whole-school community. Almost all schools have policies that prohibit the use of personal mobile phones during lessons.

Guidelines should be enforced consistently by all school staff, and supported by the school leadership team.

School staff can confiscate a mobile phone as a disciplinary penalty, and have a legal defence in respect of this in the Education and Inspections Act 2006 (s 94). Staff cannot search the contents of a pupil's mobile phone without the consent of that pupil. Where a pupil refuses to allow the contents of his/her phone to be searched, the matter can be referred to the police who have more extensive search powers. If the pupil is suspected to have committed a criminal offence, it may be advisable to involve the police from the outset.

> "I rang a parent with my mobile over a normal school matter. My mobile number was passed around and got into the hands of some teenagers who sent abusive messages."
> **A staff member**

School employees should take good care of their mobile phones. They should secure their phones when not in use, using the phone's security code. If a phone goes missing or is suspected as being stolen, it should be reported to the police and mobile operator as soon as possible, using the phone's unique International Mobile Equipment Identity, or IMEI number. This can be found printed on the phone underneath the battery, or by typing *#06# on a handset.

If it is absolutely necessary for an employee to lend a pupil a mobile phone, staff should use a school mobile rather than one owned by an individual employee. If this is not possible, the staff member should supervise the call and delete any numbers used afterwards. If being able to contact pupils by their mobile becomes necessary – for example on a school trip – school employees should use school-owned mobiles wherever possible to store numbers and contact pupils. Numbers can be deleted following the event, and learners will not have access to an employee's personal number.

Employees should be given clear guidance regarding the use of their personal mobile phone by their employer, regarding having access to pupils' numbers, storing pupils' numbers, and giving pupils access to their personal numbers.

Protecting personal information

Many school employees use the web and social networking services such as Facebook, Flickr, and Ning for work-related projects or for personal use. While school employees are private individuals, they also have professional reputations and careers to maintain. Additionally, employees are required not to do anything to endanger the health and safety of their colleagues or others.

Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff also need to be aware that many employers and other agencies now carry out web and social network service searches to find online information about staff – background, interests, career experiences and self-presentation. All staff, perhaps especially new staff in training and induction, need to be advised to ensure that information available publicly about them is accurate and appropriate.

Privacy on the internet seldom means communications are entirely private, even messaging. Think of internet communications as equivalent to sending postcards. Information sent using official school accounts or equipment will usually be accessible for monitoring purposes (this will be outlined in the school's Acceptable Use Policy) and may be requested under the Data Protection Act.

Managing personal information effectively makes it far less likely that information will be misused.

Advice for employees:

- When publishing information about yourself or having conversations with others online, it is important to be mindful of how you present yourself, who can see your content, and how you can manage this appropriately. When publishing information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer, colleague, pupil or parent, viewing your content.
- Make sure you understand who is allowed to view your content on the sites that you use – and how to restrict access to your account where necessary. If you are not clear about how to restrict access to your content to certain groups of people, regard all of your content as publicly available and act accordingly.

You can also check to see that other people aren't misrepresenting you or treating you unfairly online. If you find things you object to, you can ask the poster to take these down in the first instance. Where cases are work-related, these should be reported to your line manager or to the appropriate person as soon as possible. More serious incidents, including cyberbullying, will require a formal response from your employer, and will be dealt with within the school's disciplinary frameworks, or in more serious cases, legal frameworks.

You can check to see if others are creating or posting objectionable material about you online:

- Use search engines to check what images and text are associated with your name, or with your school and your name. This will help establish what information other people can easily find about you.
- Use search facilities within specific social networking sites – some may require you to be a logged in member.
- Staff often become aware of other people posting objectionable material about them from other learners. Encouraging everyone to report any incidents they find, rather than being a passive bystander, is an important strand of cyberbullying prevention.

'Friending' refers to the act of giving contacts permission to view information or contact you within web-based services. The terminology will vary from service to service – 'Friends' may be called contacts or connections, for example. Most social sites enable you to give different levels of access and set privacy levels on your own content and activity. These functions will vary from service to service but typically include:

- Information that is only available to the account holder
- Information that is accessible by contacts on the account holder's approved list, and
- Information that is made publicly available, either within the service or across the whole of the internet.

'Friends' does not necessarily refer in this case to people who are your actual friends, although you may choose to restrict your connections to that. 'Friends' in this context may also be work colleagues, family members, and people that you have met online.

If you have a social networking account, do not friend pupils or add them to your contact lists. You may be giving them access to personal information and allowing them to contact you inappropriately. They may also be giving you access to their personal information and activities.

If you want to use web-based social networking sites for a class or for the whole school, use a service that doesn't give contacts access to personal information and updates, or allows collaboration without requiring permissions. Alternatively ask pupils to create new, work-focused accounts for themselves, and run them as they would an online portfolio or CV.

You can find more information and advice about Social Network Services at **www.digizen.org/socialnetworking**.

Responding to incidents and reporting

School behavioural policies and procedures should explicitly refer to and outline how the school deals with cyberbullying of both pupils and staff members. Cyberbullying incidents that are targeted at school employees should be responded to in accordance with these policies and procedures.

You can find further advice about responding to and investigating incidents on the DCSF's cyberbullying guidance: **http://icanhaz.com/responding**.

- Staff should never retaliate to, i.e. personally engage with, cyberbullying incidents. They should report incidents appropriately and seek support.
- Keep any records of the abuse – text, emails, voice mail, web site or instant message. Do not delete texts or emails. Take screen prints of messages or web pages, and be careful to record the time, date and address of the site.
- Staff should inform the appropriate person (for example, their department or year head, or the designated member of senior management) at the earliest opportunity.
- Where the perpetrator is known to be a current pupil or co-worker, the majority of cases will be dealt with most effectively by the school's own mediation and disciplinary procedures.
- Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead to an identifiable individual. For instance, if another person's phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individual's phone or hacking into their IM or school email account to send harmful messages.
- If a potential criminal offence has been committed and the school is not able to identify the perpetrator, the police may 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.
- Monitoring and confiscation must be appropriate and proportionate. Parents, employees and learners should be made aware in advance of any monitoring (for example, of email or internet use) or the circumstances under which confiscation might take place.
- The designated member of the Leadership Team should contact the police where it appears that a law has been broken – for example, where death threats, assault, or other racially motivated criminal offences are involved. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police inquiries. School staff are of course able to report incidents directly to the police.
- There have been cyberbullying incidents where pupils have made unfounded, malicious claims against staff members. It is of course critical to take every claim seriously and investigate it thoroughly. In cases where an allegation is made that an employee or volunteer has: behaved in a way that has harmed or may have harmed a child; possibly committed a criminal offence against or related to a child; or behaved towards a child or children in a way that indicates s/he is unsuitable to work with children; then that allegation should be reported to the Head Teacher immediately. The Head Teacher should contact the Local Authority Designated Officer (LADO) who is responsible for providing advice and monitoring cases. The LADO will then decide whether to consult the police or children's social care colleagues. Guidance on dealing with allegations of abuse is contained in Safeguarding Children and Safer Recruitment in Education, available to download from: **http://icanhaz.com/childprotection**.

Staff should report all incidents to the designated line manager or member of their school senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, professional association, from Teacher Support Network, or other organisation.

School Employee Unions and Professional Associations

The following are members of the DCSF's Cyberbullying Taskforce:

- **Association of School and College Leaders (ASCL)**
  Phone: **0116 2991122**
  Web: **www.ascl.org.uk**
- **Association of Teachers and Lecturers (ATL)**
  Phone: **020 7930 6441**
  Web: **www.atl.org.uk**
- **National Association of Head Teachers (NAHT)**
  Phone: **01444 472472**
  Web: **www.naht.org.uk**
- **NASUWT**
  Phone: **0121 453 6150**
  Web: **www.nasuwt.org.uk**
- **National Governors' Association (NGA)**
  Phone: **0121 643 5787**
  Web: **www.nga.org.uk**
- **National Union of Teachers (NUT)**
  Phone: **020 7388 6191**
  Web: **www.teachers.org.uk**
- **Unison**
  Phone: **0845 355 0845**
  Web: **www.unison.org.uk**
- **Voice: The Union for Educational Professionals**
  Phone: **01332 372 337**
  Web: **www.voicetheunion.org.uk**

Teacher Support Network

Phone: **08000 562 561**
Web: **www.teachersupport.info**

Samaritans

Phone: **08457 90 90 90**
Email: **Jo@samaritans.org**