4. Cyberbullying: Supporting School Staff

The use of technology can provide incredible opportunities for school staff, as well as young people. It is crucial that everyone knows how to use technology responsibly. School staff should:

- be aware of what cyberbullying is.
- be clear about how they report incidents.
- know what support is in place to help them deal with incidents quickly and effectively.
- be provided with opportunities to develop their digital literacy.

Cyberbullying can seriously impact on the health, wellbeing, and self-confidence of those targeted. It may have a significant impact not only on the person being bullied, but also 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 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 who will oversee and manage the investigation and resolution of all incidents.

Staff members who are subject to cyberbullying or online abuse should:

- never personally retaliate.
- keep evidence of the incident.
- report any incident which relates to their role as a school employee to the appropriate member of staff as soon as possible.

What is cyberbullying?

Cyberbullying is **the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.**

- Cyberbullying can consist of threats, harassment, embarrassment, humiliation, defamation or impersonation.
- Cyberbullying may take the form of general insults, or prejudice-based bullying including hate crimes, for example homophobia, racism, sexism or other forms of discrimination.
- There have been cases of school employees being cyberbullied by current or ex-pupils, parents and carers, and by colleagues, as well as by people who attempt to remain anonymous.
- There are reported cases of cyberbullying involving a wide range of technologies and services, including social networking sites, apps, email, instant messaging (IM), learning environments, games and by mobile phone.

How common is cyberbullying against school employees?

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

Cyberbullying incidents can be extremely upsetting – even devastating – for the victim, whatever age they are.

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 related to cyberbullying may be criminal offences under a range of different laws.

- Cyberbullying in the form of discrimination or harassment of a member of staff may mean that the school has breached its duties under discrimination legislation.

  Schools are liable for the actions of staff members who discriminate against or harass other staff members in the course of their employment. Schools should ensure such acts are understood by their community as unacceptable. Where schools become aware that an employee has been subjected to harassment, they will need to take steps to prevent it from recurring.

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

  Staff resignation as a consequence of cyberbullying, in cases where the school has failed to take adequate steps to address the situation, may prompt claims of constructive dismissal.

- **Schools are required** to provide staff with training and information relating to abuse, including cyberbullying; have procedures in place for addressing cyberbullying incidents; and include acceptable use in relation to online and mobile communications in their staff behavioural policy.

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.

Additional Support

Staff should be aware of alternative routes they can access for additional support. These include:

- their Union or professional association
- **The Professionals Online Safety Helpline**: 0844 381 4772 **www.saferinternet.org.uk/about/helpline**
- occupational health services
- **Education Support Partnership**: Helpline: 08000 562 561 (UK-wide)
- other helplines such as the **Samaritans**

Images and Video

Employees and learners use a wide range of devices, including tablets and mobile phones, to take photographs and videos. Photo and video-sharing websites and apps are extremely popular, and are used by schools to capture learner progress, showcase events and share presentations. Employees and pupils should be informed about their rights and responsibilities regarding taking pictures and making films.

- Photos and video taken for personal use are exempt from the **Data Protection Act** (1998), for example, a parent taking photographs of a school event.
- The Data Protection Act ensures that personal information – which includes images of staff and students where they are identifiable – is processed fairly. To do this, schools should obtain consent from each student's parent and carer, and from all students who are 12 years old or over. Consent should be obtained in advance, with an explanation of why images are being taken and what they are going to be used for – especially if they are going to be published online.
- The acceptable use of equipment for creating images and film (which may most typically be mobile phones) should be covered by the appropriate behaviour policy and agreements.
- The school can request that students and staff should not take, share or publish photographs of other members of the school community without the subject's permission. Schools should clearly communicate expectations, acceptable conduct and potential sanctions regarding inappropriate image-taking and use by staff, pupils and parents.
- School-owned devices should be provided for staff members who need to take images of pupils for school purposes.
- Both pupils and employees should take care not to attach significant personal information to publicly posted information, for example full names.

Personal Mobile Devices

School employees should secure their phones when not in use, by setting up a timed lock following a short period of inactivity, and using a pin code or password. 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 necessary for an employee to lend a pupil a mobile phone, staff should use a school owned device. If being able to contact pupils by their mobile becomes necessary – for example on a school trip – school employees should only use school-owned mobiles 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. Security features, such as a time-activated PIN or passcode, should be used to ensure that if a school-owned phone is lost or stolen, content will be inaccessible.

> "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

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 web-based and social networking services for both personal and work related purposes. Some people will choose to restrict their connections to people that they know well. Many staff use online services and sites to connect to new people – for example, in order to share work and develop professional networks.

- While school employees are private individuals, they have professional reputations and careers to maintain.

  The Teachers' Standards outline the legal minimum requirements for teachers practice and conduct. Teachers, including headteachers, should safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties.

- School staff should be supported in their use of technologies including social media.

  Schools are required to ensure staff receive regular training and information relating to online safety and cyberbullying. In addition, school staff behavioural policies must include the acceptable use of technologies and the use of social media, including communications between staff and students.

  For further information about these requirements, see the Department for Education statutory guidance, **Keeping children safe in education**.

- Staff should take steps to ensure they protect their personal data.

  Staff should be aware that many employers carry out web and social network service searches to find online information about staff – background, interests, career experiences and self-presentation. All staff, including new staff in training and induction, need to be advised to ensure that publically available information about them is appropriate.

- Communications online are rarely private. Others may pass on or re-post material shared digitally.

  When posting 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 personal 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.

- Do not 'friend' current or past pupils or add them to your contact lists on personal social networking accounts.

- Information sent using official school accounts or equipment will usually be accessible to the school for monitoring purposes (this will be outlined in the schools Acceptable Use Policy), and information may also be requested under the Data Protection Act.

- 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 schools' 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:

- You can use search engines to check what images and text are associated with your name, or with a combination of your school and name. This will help establish what information other people can easily find about you.

- You can search within social networking services.

- Staff may only become aware of other people posting objectionable material when a colleague or student alerts them. Encouraging everyone to report any inappropriate material they find is an important way to address cyberbullying.

> "Unfortunately we have had incidents of inappropriate comments made about school staff members on social networking services. A Facebook and Twitter account was set up deliberately to attack the school and its staff. After consulting the Professional's Online Safety Helpline, we were successful in our dealings with Twitter to get the site taken down and with Facebook to remove the school's branding. We were quick to move when alerted to this content, giving strict instructions to staff not to engage with these individuals online which I am sure stopped the problem escalating."
> e-Safety Co-ordinator, secondary school