Department for Education

Cyberbullying: Advice for headteachers and school staff

Who is this advice for?

This is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

Overview

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. It is important that schools take measures to prevent and tackle bullying among pupils. But it is equally important that schools make it clear that bullying of staff, whether by pupils, parents or colleagues, is unacceptable. Evidence indicates that one in five (21%) teachers have reported having derogatory comments posted about them on social media sites from both parents and children.

School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyberbullying and should work together to create an environment in which pupils can learn and develop and staff can have fulfilling careers free from harassment and bullying.

Schools can offer support to parents on how to help their children engage safely and responsibly with social media, perhaps through a parents' evening, advice in a school newsletter or signposting to other sources of support and advice. Creating a good school-parent relationship can help create an atmosphere of trust that encourages parents to raise concerns in an appropriate manner. Part of this is making sure that parents and carers are aware and understand how to communicate with the school. Schools should also make clear that it is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face.

Schools should encourage all members of the school community including parents to use social media responsibly. Parents have a right to raise concerns about the education of their child, but they should do so in an appropriate manner.

School staff

All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times. Here is some key advice for staff which may help protect their online reputation:

- Ensure you understand your school's policies on the use of social media, Childnet's 'Using Technology' guide has more information on what to be aware of.
- Do not leave a computer or any other device logged in when you are away from your desk.
- Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by pupils.

Published: November 2014

- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the Safer internet advice and resources for parents and carers.
- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation minisite has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not accept friend requests from pupils past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school's contact details. On school trips, staff should have a school mobile phone rather than having to rely on their own.
- Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

If you are bullied online

- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.

Employers have a duty to support staff and no-one should feel victimised in the workplace. Staff should seek support from the senior management team, and their union representative if they are a member.

The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

Schools

Whole-school policies and practices designed to combat bullying, including cyberbullying, should be developed by and for the whole school community. All employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff and supporting them if it happens.

Schools should develop clear guidance to help 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. Kidscape has also produced best practice advice and guidelines for professionals. The Diana Award also runs a whole school Anti-Bullying Programme, information and good practice can be found at www.antibullyingpro.com.

Reporting

The whole school community should understand reporting routes and responsibilities. Many schools will appoint a designated person to deal with bullying while others will distribute responsibility among a number of staff.

Acceptable use policies

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

- Rules on the use of school equipment, software and access routes when used on or off the school premises within school hours: for example, internet access, tablets, lap tops and mobile phones.
- Acceptable behaviour for pupils and employees, including behaviour outside school: for example teachers' and pupils' use of social networking services and other sites, so as not to harm others or bring the school into disrepute.
- School staff should expect the school to react quickly to reported incidents or support the member of staff concerned to do so. It is also important that staff who are harassed in this way receive support and information enabling them to access appropriate personal support. The school should endeavour to approach internet

providers or other agencies on their behalf in order to request that the inappropriate material is removed. The internet provider may only accept a request from the victim. However, the school may want to take action if it is on a school website or email address.

- If it is necessary for the person being bullied to contact the service providers directly, the school may provide support. This might apply, for example, in cases of identity theft, impersonation or abuse via a mobile phone service.

Useful resources

The Parent Zone has established a training programme designed to enable schools and professionals working with parents to deliver their own sessions on internet safety. They also provide innovative resources for schools to help and support parents, particularly around e-safety.

Facebook has produced Empowering Educators support sheet specifically for teachers and launched the Bullying Prevention Hub with Yale's Centre for Emotional Intelligence.

Getting offensive content taken down

If online content is offensive or inappropriate, and the person or people responsible are known, you need to ensure they understand why the material is unacceptable or offensive and request they remove it.

Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report.

Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is; for example by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site’s terms and conditions. Where the material is suspected of being illegal you should contact the police directly.

Contact details for social networking sites

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools.

Social networking site	Useful links
Ask.fm	Read Ask.fm's 'terms of service' Read Ask.fm's safety tips **Reporting on Ask.fm:** You do not need to be logged into the site (i.e. a user) to report. When you move your mouse over any post on someone else's profile, you will see an option to like the post and also a drop down arrow which allows you to report the post.
BBM	Read BBM rules and safety
Facebook	Read Facebook's rules Report to Facebook Facebook Safety Centre
Instagram	Read Instagram's rules Report to Instagram Instagram Safety Centre
Kik Messenger	Read Kik's rules Report to Kik Kik Help Centre
Snapchat	Read Snapchat rules Report to Snapchat Read Snapchat's safety tips for parents
Tumblr	Read Tumblr's rules Report to Tumblr by email If you email Tumblr take a screen shot as evidence and attach it to your email
Twitter	Read Twitter's rules Report to Twitter
Vine	Read Vine's rules Contacting Vine and reporting
YouTube	Read YouTube's rules Report to YouTube YouTube Safety Centre

Mobile phones

All UK mobile phone providers have malicious or nuisance call, text or picture message centres set up and have procedures in place to deal with such instances. If you are being bullied they will help you to change your number if necessary. If you want to prosecute the perpetrator contact the police. The mobile provider will work closely with the police and can usually trace malicious calls for them.

Service providers:

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	4445 or 202	08705 678 678	0870 241 0202
VodaFone	191	03333 040 191	03333 048 069
3	333	08433 733 333	08433 733 333
EE	150	0800 956 6000	0800 956 6000
Orange	150	07973 100 450	07973 100 150
T-Mobile	150	07953 966 150	07953 966 150
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Reference: DFE-00652-2014