LEWES OLD GRAMMAR SCHOOL

Cyber-bullying Guidance

this guidance should be read in conjunction with the

School's Anti-Bullying policy

Cyber-Bullying Guidance

What is cyberbullying?

So what is cyberbullying? The simple answer is bullying by means of electronic media. The Goldsmiths survey identified seven means: text message; mobile phone pictures/video-clips (including 'happy slapping' - filming violent physical attacks); mobile phone calls; email; chat rooms; instant messaging, and websites (blogs, personal websites, social networking sites, etc., on which comments about others are posted - for example, Bebo, Youtube and Ratemyteacher, to name but three). In the words of the DfES(4), it "*adds a new and worrying dimension to the problem of bullying - there's no safe haven for the person being bullied. Unlike other forms of bullying, cyberbullying can follow people into their private spaces and outside school hours. Cyberbullies can communicate their messages to a wide audience with remarkable speed, and can often remain unidentifiable and unseen*". It therefore presents particular and difficult challenges to schools.

What are the legal issues that arise?

The legal issues that may be of relevance in relation to cyberbullying (both of pupils and teachers) are numerous.

- Schools have a statutory duty to make arrangements to safeguard and promote the welfare of the children that are its pupils;
- Schools also owe a common law duty to take reasonable steps to protect the health and safety of their pupils and their employees;
- Certain legal obligations that arise from the contract with parents and with employees may come into play (for example, to have responsibility for the care of pupils; to follow a particular procedure such as a parental complaints procedure or an employee grievance procedure);
- There is of course law relating to confidentiality, data protection and monitoring of electronic communications;
- In some circumstances, the law of defamation might be relevant, given that cyberbullying can include publication of comments about people;
- Discrimination law (including harassment) may also be relevant;
- Some criminal offences may apply, for example harassment under The Protection from Harassment Act 1997;
- Grooming, where an individual meets or travels to meet with an under 16 year old to commit a relevant offence if the individual has communicated with the child twice, is a criminal offence under the Sexual Offences Act 2003;

- There are certain procedural requirements when dealing with parental or employee complaints and instances of pupil misconduct, including the fundamental principles of natural justice;
- Recent legislation may also have a bearing. For example, The Education and Inspections Act 2006 recently introduced a statutory defence to allegations of seizure, retention, etc., where property (e.g., mobile phones) is confiscated in certain circumstances.

That list is not exhaustive, and it is beyond the scope of this article to delve deeper into the (sometimes complex) legal issues that arise. Suffice to say that schools need to consider their legal obligations and responsibilities when dealing with cyberbullying and the claims that may arise in the event that those obligations are breached (some of which may prove to be extremely costly), as well as the various means by which the law assists schools in tackling cyberbullying.

They also of course need to consider the possibility of intensive and potentially damaging media attention, a very real risk particularly in light of the extensive interest in this area at the moment.

What should schools do?

What then should schools be doing about this seemingly growing and distinctively 21st century problem? The answers can perhaps be divided into two categories: steps to prevent and limit cyberbullying and steps to take in response to specific instances of cyberbullying.

Preventative steps

Turning first to some steps that might be taken to prevent (or, perhaps more realistically, limit) cyberbullying.

- Create/review/develop (as the case may be) a comprehensive anti-bullying policy that covers cyberbullying and similarly ensure that cyberbullying is addressed in school training and awareness campaigns about bullying in general;

- Establish clear guidelines about the use of mobile phones and computers both in school and at home. Those guidelines might appear in a number of different forms, for example, school rules and an acceptable use policy, to name but two. They should set out the standards of use and behaviour that the school expects, the sanctions that may be applied (including confiscation), and the procedures and support strategies that will be employed for dealing with misuse. The guidelines should be wide enough to cover use of phones and computers both at home and in school: indeed, given that the pro blem of cyberbullying is not limited to school time - the Goldsmiths survey found that there was more cyberbullying out of school than in - it is critical that parents as well as pupils are aware of such guidelines and their responsibilities in helping deal with the problem;

- Regularly review IT security measures - firewalls, password protection, anti-virus protection, filtering systems and so on. Ensure that all users are aware of the importance of such measures and their obligations to protect security and confidentiality;

- Consider designating one of the senior management team the internet safety coordinator to act as a central point of contact for all internet safety issues within the school;

- Monitoring of email traffic and internet use will certainly play a role in policing and discouraging cyberbullying. However, great care needs to be taken because of the legal restrictions and responsibilities in this area. It is beyond the scope of this article to give detailed advice in relation to monitoring, but the basic principles are to ensure that parents, pupils, teachers and other users of the school network are aware that internet use and emails may be monitored, that monitoring is carried out for legitimate reasons and is proportionate (i.e., only goes so far as is necessary and is carried out in such a way that the potential intrusion on privacy is limited);

- If possible, provide pupils and employees with access to some sort of confidential counselling service;

- Put in place measures for dealing with media interest should the worst case scenario materialise. For example, ensure that there is a plan for handling press interest and that your key staff know how to react in the event that the press call or arrive at the gate;

- Review the DfES guidance in relation to this topic (see footnote 4 for the link). The internet is also a source of various model policies. See for example the Becta website (http://schools.becta.org.uk/index.php?section=is).

Reactive steps

No matter the extent of the preventative measures you take, there will undoubtedly be times when you will face instances of cyberbullying of both pupils and teachers.

How you react will of course depend on the particular circumstances of each individual case, but below is a checklist of measures that you should consider taking.

- Take allegations and complaints seriously. Consider whether it is appropriate to deal with them informally or formally;

- Consider at the outset whether it is appropriate to involve social services and/or the police. This is very much a decision that will have to be taken depending on the particular circumstances at the time and specifically whether there is any potential for a crime having been committed or for a child being at risk, but a very general rule would be to make contact (albeit possibly anonymously initially) if there is an element of doubt as to whether you should. If you make contact and they are interested, keep them informed and work with them: their involvement may well have an impact on the way you deal with the matter internally;

- Find out the facts so far as possible and do so as soon as possible. Appoint an appropriate person to carry out an investigation. That said, in instances where there may have been a misuse of computers and there is a possibility of involving the police and/or social services, isolate the computers concerned and do not allow anyone to access them until the police/social services have given the green light, since any interference with a computer can fundamentally flaw a case against a defendant;

- Consider whether any immediate technical measures can or should be taken (such as preventing access to a particular site or temporary withdrawal of internet access). These are steps which many schools are, rightly, reluctant to take partly on wider educational grounds but also given that the internet is now embedded in the curriculum as a learning tool. However, in certain circumstances there may be no other option;

- Think carefully about who needs to be informed - parents of children concerned, for example - and about what they need to know. Only inform those it is necessary to inform and ensure that information is kept confidential, so far as reasonably possible;

- Keep records of conversations, investigations etc.;

- Be mindful of procedural requirements in, for example, dealing with a grievance or a potential expulsion situation;

If the case involves rogue/spoof/protest/hate websites, consider approaching the Internet Service Provider, but bear in mind that some ISPs will (legitimately) refuse to cooperate in, for example, tracing an author until proceedings are issued. Also bear in mind that attempting to take action may simply give encouragement to the author;

- U.S.-based sites are required by law to operate a 'three strikes and you are out' policy: if users have three complaints made against them, not only are their postings removed but their accounts are cancelled and they are banned from using the site. If it is a popular site (such as facebook.com, for example, who do have a 'Repeat Infringer Policy'), the fear of a ban could be a deterrent to users.

It is almost certainly the case that other forms of bullying are still more common than cyberbullying, but there is no doubt that it is an increasing and significant problem for schools, parents, pupils and staff alike and one that schools can ill-afford to ignore. Perhaps one of the keys to minimising instances of it is to ensure that all such parties are, so far as possible, involved in and committed to tackling the problem together.

Additional Information

DfES guidance on cyber-bullying entitled "Don't suffer in silence" - www.dfes.gov.uk/bullying/cyberbullying

Recommended review period: Annual
Review by: Head, Assistant Head Pastoral, DSL, Bursar
Date reviewed: August 2017
Date to be reviewed: August 2018