



BOARDING BRIEFING PAPER 23

APRIL 2008

CYBERBULLYING

The legal implications and consequences

by

Christine Betts

Senior Lawyer, Veale-Wasbrough Lawyers

The Boarding Schools' Association
Grosvenor Gardens House
35-37, Grosvenor Gardens, London SW1W 0BS
Tel : 020 7798 1580 Fax : 020 7798 1581
e-mail : bsa@boarding.org.uk
website: www.boarding.org.uk

Duties for Schools

Bullying of any kind is an important safeguarding issue for schools. Schools have always had a common law duty of care towards pupils. This has been codified in the Education Act 2002 and the Education (Independent Schools Standards) (England) Regulations 2003 and is now known as the duty to safeguard and promote the welfare of children. Schools are required to have anti-bullying policies in place which comply with government guidance. Standard 2 of the National Minimum Standards for Boarding Schools requires "an effective policy on countering bullying, which is known to parents, boarders and staff and which is implemented successfully in practice".

Current anti-bullying policies need to be updated to include references to cyberbullying but it is also important to have a separate policy focusing specifically on cyberbullying because of the important differences between traditional bullying and cyberbullying. This can be combined with an "Acceptable Use Policy" setting out a more positive framework for the use of technology by pupils.

Negligent handling of bullying which results in pupils suffering harm may lead to claims for compensation. There are limitation periods on claims which generally vary from 3 years to 6 years after the child reaches 18. In very exceptional cases the courts can extend these limits.

This Briefing Paper focuses on cyberbullying of pupils although it is recognised that staff can be the victims of cyberbullying, causing stress and breakdown and that school employers have similar protective duties towards staff.

What is cyberbullying?

There can be very few Heads and teachers who do not recognise the term "cyberbullying". It is such a widespread phenomenon that the Department for Children, Schools & Families (DCSF) has a Cyberbullying Taskforce which includes representatives from:

- the Anti-Bullying Alliance (founded by the NSPCC and National Children's Bureau in 2002)
- teachers' professional associations
- mobile 'phone companies
- Internet Service Providers
- government departments.

The DCSF has commissioned Childnet International, a registered charity committed to extending the benefits of the internet for children, to develop detailed guidance for schools in consultation with the Cyberbullying Taskforce. The guidance, "Cyberbullying: Safe to Learn: embedding anti-bullying work in schools" (DCSF - 00658-2007), was published in September 2007 and can be accessed from www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying.

The DCSF guidance offers the following definition of cyberbullying:

"The use of Information & Communications Technology (ICT), particularly mobile 'phones and the internet, deliberately to upset someone else".

Examples reported by schools include:

- pupils who set up website pages and invite others to post derogatory comments about a pupil;
- pupils who film fights or assaults (so-called "happy slapping") and circulate them via mobile 'phones;
- pupils sending insulting and vicious text messages;
- pupils posting fake and obscene photographs of the victim on a social networking site;

- pupils hacking into social networking sites and removing and circulating material which may be embarrassing or personal.

What makes cyberbullying different from "ordinary" bullying?

It can be argued that cyberbullying is just bullying. Schools should certainly not hold back from dealing with bullying incidents just because, for example, a pupil uses a home computer to harass a fellow pupil rather than passing scurrilous notes around the class in the traditional manner.

However, cyberbullying can have far greater impact because of a number of factors including:

- invasion of personal space;
- the anonymity (at least initially) of the bully;
- the ability to broadcast upsetting messages and images rapidly to a potentially huge audience and to continue to do so repeatedly over a long period of time.

Another unusual factor is the way that other pupils who would not normally take part in bullying behaviour may be drawn in as accessories. This can happen, for example, when an image is circulated on a mobile 'phone by a bully and recipients extend the circulation further by passing it on to a wider circle.

Are cyberbullies breaking the law?

Pupils are entitled to their freedom of expression and respect for their private lives, provided they do not infringe the rights of others. Infringement includes libel and slander (defamation), bullying, harassment and victimisation, inciting hatred on racial, religious or homophobic grounds (hate crimes), breach of confidentiality, breach of copyright or the school's trade mark, child pornography and a wide range of other criminal offences.

There are a number of offences (both civil and criminal) that may be committed in the course of cyberbullying. Some may be covered by more than one piece of legislation. It should be noted that the age of the perpetrator is not relevant although the general age of criminal responsibility (10 years) applies and prosecutions are unlikely for children under 14.

Obscene Publications Act 1959 makes it an offence to "publish" an obscene article (which can include written material, photographs or films). Publishing includes circulating, showing or transmitting the article.

Protection of Children Act 1978 makes it an offence to take an indecent photograph (or film) of a child. A "child" is anyone under 18 although there are defences involving children over 16 in a marital (or similar) relationship. The definition of "photograph" includes images on a mobile phone or stored on a computer and also includes "pseudo-photographs" where images have been manipulated. It is also an offence for someone to distribute or show such images or to have them in his possession with the intention of showing them to himself or others.

Public Order Act 1986 makes it an offence to use threatening, abusive or insulting words, behaviour and images with the intention to cause harassment, alarm or distress. This can apply where a mobile 'phone is used as a camera or video.

Malicious Communications Act 1988 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.

Computer Misuse Act 1990 makes hacking into computer accounts an offence.

Protection from Harassment Act 1997 creates both civil and criminal offences of harassment. Harassment is defined as a course of conduct which causes alarm or distress. This means that there must be repeated incidents (more than twice). It is also an offence to cause another person to fear, on at least two occasions, that violence will be used against them.

Communications Act 2003 makes it an offence to send a grossly offensive, obscene, indecent or menacing communication. There is also an offence of sending a message that is known to be false for the purposes of causing annoyance, inconvenience or needless anxiety.

The consequences of being prosecuted for such offences may be far-reaching. Convictions for some of these offences may carry the requirement to sign the Sex Offenders Register and even cautions for such offences may also affect the ability of the offender to enter a career working with children or "vulnerable adults."

The law of defamation is also relevant. Someone who publishes material which is damaging to the reputation of an individual or a company may be sued for compensation.

Young people who use their mobile phones or other devices to record physical attacks can be prosecuted as accessories to serious criminal offences. In February 2008 a 15-year-old girl was convicted of aiding and abetting manslaughter when she filmed a man being beaten up by two youths. The man subsequently died of his injuries. The girl was sentenced to be detained in a young offenders' institution for two years.

What should schools be doing about cyberbullying?

It must be recognised that use of mobile phones, the internet and a growing range of electronic devices is firmly embedded in the culture for young people and can bring many benefits if properly managed. Simple and general prohibition of the use of these devices would be unenforceable and unlikely to be supported by parents.

Preventive measures

Schools need to have proactive strategies to prevent cyberbullying as well as dealing with incidents as they happen. Schools must seek to create a culture where cyberbullying is widely regarded as unacceptable by means of a clear policy, firm rules and reinforcement of the core values of trust and respect, with disciplinary sanctions and permanent exclusion in reserve.

A separate policy on cyberbullying together with an Acceptable Use Policy should be developed in full consultation with pupils, staff (in particular IT staff) and parents. A policy on cyberbullying should make it clear that:

- the school reserves the right to monitor pupils' use of the internet on a routine basis and to examine mobile phones where there is reason to suspect abuse;
- misuse of technology is subject to the school's disciplinary regime;
- pupils will be held personally responsible for all material they have placed on a web site and for all material that appears on a web site of which they are the account holder;
- misconduct of this kind outside school will be amenable to school discipline if the welfare of other pupils or the culture or reputation of the school are placed at risk; and
- sanctions may include confiscation of mobile phones or restrictions on the use of the internet.

The policy should be published to all parents and summarised for the school rules. There should be an expectation that pupils will report every breach of the policy.

The policy will need to be driven vertically and horizontally throughout the school in staff meetings, school assemblies, house assemblies, IT lessons, PHSE lessons and by all the other usual methods, and referred to in the standard anti-bullying policy. Schools also need to ensure they keep up to date with technological developments and that this is reflected in the regular monitoring and updating of the policy. The DCSF has stated that it will regularly update its guidance to schools. Schools may find it helpful to give a senior member of staff the responsibility for reviewing the policy in the light of such guidance.

In addition to the policy, schools should find ways of providing constructive messages to young

people to help them to protect themselves. For example the Information Commissioner publishes material on his website (www.ico.gov.uk) aimed specifically at young people which gives advice on protecting their personal information on networking sites. External speakers could also be brought in to lead discussions and demonstrate new technology, showing that the school is taking a positive attitude to technology and developing more trust with pupils as a result.

The policy should include clear routes for victims (or witnesses) to report incidents confidentially to staff. Victims of cyberbullying need to be encouraged to report incidents as soon as possible and to hand evidence over to staff. Schools need to devise ways of supporting victims who may fear reprisals or may even believe that they are partly to blame for what has happened to them. If potential victims are confident that they will be protected, this can act as a deterrent against bullying of any kind.

An Acceptable Use Policy should include rules which:

- encourage responsible use of the internet and other electronic devices for educational purposes;
- emphasise the importance of keeping passwords and login names confidential;
- prevent the downloading of unsuitable material;
- protect the security of the school's computer system by taking precautions against viruses;
- prohibit plagiarism by use of internet material; and
- prohibit hacking.

Responding to incidents

It may be helpful to see incidents as potential child abuse and therefore to use the school's child protection procedures as guidance in responding to cyberbullying. Key factors in common will be:

- reassurance for the victim (with cyberbullying, this can include advice on self-protection measures such as blocking messages from a particular source or cleaning up "buddy lists");
- the need to preserve evidence in the form of text messages, images and other material;
- avoiding leading questions and taking care to ensure that an initial investigation will not prejudice any later legal proceedings should these become necessary; and
- dealing with the matter discreetly but giving no guarantee of full confidentiality in case matters need to go further.

However, there are other elements unique to cyberbullying. These include the potential difficulty of identifying a perpetrator who may be using an internet pseudonym or has appropriated another person's mobile phone for the purposes of sending abusive messages. There are ways of identifying perpetrators. Whilst many people believe that they can post offensive messages with complete anonymity, this is not the case. A recent case has confirmed that the courts can and will order websites to disclose the identity of someone who has posted offensive and defamatory material.

In *Sheffield Wednesday Football Club v Hargreaves* [2007] EWHC 2374 (QB) angry fans of Sheffield Wednesday Football Club had, using pseudonyms, posted malicious allegations against the club's management team on a website. The judge agreed to order disclosure of the fans' identities because their postings "*might reasonably be understood to allege greed, selfishness, untrustworthiness and dishonest behaviour*". However, he ruled that other fans should retain their anonymity as their postings were more trivial or likely to be understood as jokes.

Serious cases may need to be referred to the police for investigation. The police will have more resources at their disposal for investigation, but only the most serious cases are likely to be given priority and such investigations may take a considerable amount of time. However, in many cases,

conventional methods of investigation by the school, such as observation by staff or statements from witnesses, may be successful in identifying perpetrators.

Disciplinary action

Normal disciplinary procedures need to be followed and alleged perpetrators should be dealt with fairly. Some more naïve pupils may not realise the seriousness of apparently low-level behaviour such as passing on a copy of an offensive message to a friend. However, it needs to be made clear that, in terms of the impact on the victim and on the school community, anyone who participates in the dissemination of offensive material is supporting and reinforcing unacceptable behaviour.

Schools are entitled to use the full range of sanctions available under their behaviour policies. Punishments that fit the crime, such as restricting or prohibiting the use of technological devices either temporarily or indefinitely, may have the most impact. Contrary to views sometimes expressed by pupils and, sadly, parents, possessing or using a mobile phone is not a "human right" under the European Convention.

There are provisions in the Education and Inspections Act 2006 which are aimed at clarifying some grey areas that have developed, particularly in the maintained sector, as to the legal powers of a school to enforce disciplinary measures. Independent schools have always had the power to operate a disciplinary regime which includes reasonable measures such as confiscation. Parents sign up to this regime on entering a contract with the school when their child is admitted. The 2006 Act provisions should be helpful, however, if disagreement arises or a parent makes a complaint about a particular sanction.

In summary, section 91 of the Act declares that the imposition of a disciplinary penalty will be lawful if three conditions are met:

1. that the penalty is not prohibited by law (as with, for example, corporal punishment) and is reasonable in all the circumstances;
2. that the decision to impose the penalty is made by either by a paid member of staff who is not prohibited by the Head from imposing such a penalty or by any other member of staff who is authorised to do by the Head and it is reasonable for the Head to have done so; and
3. that the decision to impose the penalty is taken either when the pupil is on school premises or elsewhere when the pupil is under the lawful control of a member of staff.

Section 94 provides a specific defence to any action following confiscation where the member of staff can show that the confiscation was lawful either under section 91 or in any other way. This can include confiscation of a mobile phone where it is being used in contravention of the school behaviour or anti-bullying policy.

Suspension (or fixed-term exclusion) should always be used sparingly, but it may be necessary to protect witnesses or preserve evidence during an investigation as well as a disciplinary sanction in its own right. Expulsion (permanent exclusion) should be a last resort and used in the most serious cases only, but will send a clear message that cyberbullying will not be tolerated.

National Minimum Standard 4.6 requires major punishments to be recorded in a suitable book or log. Examples of major punishments include punishments for offences which "would constitute criminal behaviour in the case of an adult." As explained above, the criminal offences that may be committed as part of cyberbullying are criminal behaviour whatever the age of the perpetrator.

External reporting

Schools should be capable of dealing with most cases of cyberbullying through internal procedures. However, as already mentioned, more serious cases may need to be referred to the police. This will usually be where it is apparent that a criminal offence as detailed above has been committed, although there are other factors as well (see below). Referral to the police will usually result in a joint investigation with social services (and vice versa).

There is no obligation on the school to report suspicions of a criminal offence. This is a wide-reaching decision and schools will be justified in giving the matter very full consideration before a report is made. The victim and his or her parents should be consulted although their views may need to be overridden in the interests of the school community.

The decision to refer is a matter of judgement for the school. Schools are strongly advised to make a referral if any of the following factors are present:

- there is evidence that a serious criminal offence has been, or is about to be, committed;
- the victim has suffered significant harm or is at risk of significant harm (including self-harm);
- there is evidence or suspicion of adult involvement - schools need to be aware of the possibility that abuse and manipulation of children via the internet may involve adults posing as children, even as other pupils;
- there is evidence or suspicion of concerted action by a group of pupils, particularly if more than one school is involved;
- any of the children involved are on the Child Protection Register.

If there is room for doubt over a referral to either the police or social services, the school should discuss the matter with the Local Authority Designated Officer for Child Protection (LADO), on a "no-names" basis if necessary or take legal advice.

If the school decides not to refer to the police or social services, the decision-making process should be recorded and the parents should be informed of their rights to take the matter further if they wish. If there is a police investigation, the school can request that any interviews of pupils or staff should take place away from school premises or that only non-uniformed officers attend the school.

Responsibility for inspection of the welfare aspects of boarding schools passed from the Commission for Social Care Inspection (CSCI) to Ofsted on 1 April 2007. Ofsted may expect a major incident such as a police or social services investigation to be reported to them.

Summary of Key Points

Schools have legal duties to safeguard and promote the welfare of children in their care. These include specific duties to address bullying. Cyberbullying is a particularly pernicious aspect of bullying in schools and is recognised as posing significant risks to the welfare of children.

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

The Department for Children, Schools and Families has published detailed guidance: "Cyberbullying: Safe to Learn: embedding anti-bullying work in schools" (DCSF - 00658-2007) which can be accessed from www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying.

A number of criminal offences can be committed in the course of cyberbullying. These include:

- harassment
- publishing obscene material
- taking, storing and circulating indecent images of children
- using threatening, abusive or insulting behaviour
- aiding and abetting crimes of violence.

Perpetrators may also be liable for defamation by circulating material which damages a person's reputation.

Preventive measures should include:

- raising awareness of the issue throughout the school
- updating existing anti-bullying policies to refer to cyberbullying
- drawing up a separate policy on cyberbullying
- drawing up an "Acceptable Use Policy"
- providing confidential reporting procedures for victims and witnesses.

Response to incidents should include:

- support for victims
- careful investigation procedures
- constructive but firm disciplinary action
- assessment of risk and referral of serious cases to police or social services.