

Cyberbullying in the UK: Legal aspects and good practice

Marczak, M.

Published poster deposited in Coventry University Repository

Original citation:

Marczak, M. (2010) Cyberbullying in the UK: Legal aspects and good practice [poster]. Given at COST ACTION IS0801: Workshop 2: The legal aspects of cyberbullying, 2010, Antwerp, Belgium.

<https://antibullyinglaws.files.wordpress.com/2014/01/cyberbullying.pdf>

<https://sites.google.com/site/costis0801/>

Copyright © and Moral Rights are retained by the author(s) and/ or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This item cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder(s). The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders.

Magdalena Marczak, The University of Nottingham, IWHO
 Dr Iain Coyne, The University of Nottingham, IWHO

This poster outlines the legal, regulatory and good practice framework for controlling cyberbullying in UK educational contexts. Currently, in the UK cyberbullying per se is not a specific criminal offence however it could be a criminal offence under a number of laws.

Law	Year	Legal aspect	Best Practice
The Protection from Harassment Act	1988	Relevant for incidents that have happened repeatedly (i.e. on more than two occasions). Section 1 prohibits behaviour amounting to harassment of another. Section 2 provides a criminal offence and section 3 provides a civil remedy for breach of the prohibition on harassment in section 1. Section 4 provides a more serious offence of someone causing another person to fear, on at least two occasions, that violence will be used against them.	The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.
The Communication Act	2003 s.127	Section 127 covers all forms of public communications, and subsection (2) defines an offence of sending a 'grossly offensive...obscene, indecent or menacing' communication.	Subsection (2) defines a separate offence where for the purposes of causing annoyance, inconvenience or needless anxiety, a person sends a message which that person knows to be false (or causes it to be sent) or persistently makes use of a public communications system.
The Public Order Act	1986	Section 5 makes it an offence to, with the intent to cause harassment, alarm and distress, use threatening, abusive or insulting words, behaviour, writing, signs or other visual representation within the sight or hearing of a person likely to be caused harassment, alarm or distress.	This offence may apply where a mobile phone is used as a camera or video rather than where speech writing or images are transmitted.
The Malicious Communications Act	1988	Section 1 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.	Under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent offensive or threatening. Such offence is punishable with up to six months imprisonment and/or a fine of up to £5000.
The Obscene Publication Act	1959	It is an offence under this Act to publish an obscene article.	Publishing includes circulating, showing, playing or projecting the article or transmitting that data, for example over a school intranet. An obscene article is one whose effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it.
The Computer Misuse Act	1990	When cyberbullying takes the form of hacking into someone else's account.	Examples of how hacking can be used to cyberbully include: - accessing and copying someone's information (i.e. emails or pictures) in order to harass or humiliate them. This could include posting private information on public sites, emailing or forwarding data by mobile phone, or printing and circulating paper copies. - deleting someone's information – for example, electronically submitted or stored assignments, school/academic homework or emails. - impersonating someone whose account has been hacked in order to post abusive comments. This might include posting messages to the school's Virtual Learning Environment (VLE), sending Instant Messages or emails, or may involve using someone's mobile phone to send abusive calls, texts or images.
The Defamation Acts	1952 & 1996	It applies to any published material that damages the reputation of an individual or an organisation, and it includes material published on the internet.	Where defamatory material is posted on a website the person affected can inform the host of its contents and ask the host to remove it. Once the host knows that the material is there and that it may be defamatory, it can no longer rely on the defence of innocent dissemination in the Defamation Act 1996. This means that the person affected could (if the material has been published in England and Wales) obtain a court order to require removal of the material, and could sue either the host or the person who posted the material for defamation.
The School Standards and Framework Act	1998	Places a specific duty on state-maintained schools to combat bullying. Ensures that anti-bullying procedures are in place in state-maintained schools.	Pupils and parents need to know what pupils' responsibilities are in the use of information communications technology (ICT), and what sanctions will be imposed for misuse. Pupils and parents must also be aware that the school now has a statutory obligation under the Education and Inspections Act 2006 to provide them with support if the cyberbullying takes place outside school.
The Education (Independent Schools Standards) Regulations	2003	Places a specific duty on independent schools to combat bullying. Ensures that anti-bullying procedures are in place.	These regulations ensure staff have an opportunity for discussing counter-bullying strategies and reviewing them, determine the strategies and procedures, ensure appropriate training is available and that these procedures are brought to the attention of staff pupils and parents.
The Education and Inspections Act	2006	Headteachers have the power to regulate the conduct of pupils when not on school premises or not under the control of a member of staff, to 'such an extent as is reasonable'.	The act also provides a defence for school staff in confiscating items such as mobile phones from pupils. A pupil can be requested to reveal a message, or content on their phone, to establish if bullying has occurred. Disciplinary measures may be taken against those who refuse to comply.

1. Is there a need for a cyberbullying law?
2. What should be covered in a cyberbullying law that is beyond existing laws?
3. How much use is made of current laws for cyberbullying cases?
4. What would be the unintended impact of a cyberbullying law?

