Cyberbullying – Factsheet

Version	Date	Author	Changes
1.0	Jan 2020	B. Ewing	New Version
Board Approved: February 2020			

What is Cyberbullying?

Defined as – the Use of technology, e.g. mobile phones/internet, to deliberately upset someone.

Cyberbullying can be used for all other types of bullying but uses technology as a tool. It can include a range of unacceptable behaviour, including harassment, threats and insults.

Cyberbullying can be an extension of face to face bullying, as another route for harassment. It does differ in several ways to other methods, e.g. remote invasion, messages difficult to control, different profiles for bully and target. While bullying behaviour may not be criminal, there are laws that can apply to harassment and threats.

Forms of Cyberbullying

Threats of intimidation - Serious threats can be sent by mobile phone, email and via comments on websites, social networking sites or message boards.

Harassment or stalking - Repeated, prolonged unwanted texting, whether explicitly offensive or not, is harassment. Online stalking (cyberstalking) where a person's online activities are repeatedly monitored, can cause psychological harm and fear. Previously safe enjoyable environments can become threatening, and online activity may lead to anxiety.

Online harassment and stalking can take many or multiple forms, and may be a continuation of offline bullying behaviour or lead to offline bullying. Forms of harassment include:

- Repeated unwanted messages, or calls, including silent calls.
- Repeated harassment on public forums, or derogatory or defamatory statements to provoke a response ('flaming').
- Tracking targets by using spyware
- Sending viruses

Vilification / defamation - Cyberbullying can include posting upsetting or defamatory remarks about a person online, or name-calling using technology. Insults could be general, or prejudice-based. Sexist, homophobic and racist messages or attacks on other types of difference are common- a disability, background, appearance or socio-economic position.

Ostracising / peer rejection / exclusion - Online exclusion can be harder to detect than offline when others are present. Social network sites provide a platform to establish online presence and talk to others. They can extend one's social space and activity. Most social networks function as gated communities, limited to members, so only a few sites may be popular to a group of rowers. It is possible for them to set up a closed group, which can protect them from unwanted intrusion. It also means that excluding someone- by refusing to respond to messages, or deleting them from lists- can be hurtful. Though boundaries about acceptable behaviour are essential from the beginning and breaches of this online code of behaviour may lead to an individual being excluded by the group administrator.

Identity theft / unauthorised access / impersonation - Hacking generally means gaining access to an account by finding out or guessing their username and password. Hacking into systems, accounts or files is not always cyberbullying, but is always serious. Hacking is illegal, and examples of how it can become cyberbullying include:

Accessing and copying personal information, e.g. emails or pictures, to harass or humiliate, posting private information on public sites, forwarding data, or printing and circulating.

Deleting personal information – e.g. electronic training programmes, or important emails.

Impersonating someone – e.g. pretending to be a person whose account has been hacked, in order to post abuse. This may include sending instant messages, or using someone's phone to send abusive calls, texts or images.

Publicly transmitting personal or private data - Once electronic data is made public, it is hard to contain. It can be passed between devices wirelessly, sent by text or email, uploaded to websites or video hosting sites. 'Happy slapping' refers to physical assaults recorded and circulated by phone. Those who record an attack can be involved in cyberbullying. Circulating images of attacks can be harassment, and will often compound the original harm. Creating, possessing copying or distributing indecent images of those under 18 is illegal, even if done for fun or with consent. Please also see PSNI guidance on [sexting](). This also applied to indecent 'pseudo-photos'- images created or adapted using software.

Manipulation - This is an under considered form of bullying, e.g. applied pressure to reveal personal information or to arrange a physical meeting. Online friendship status may be used. Manipulation is difficult to detect, as the victim often feels implicated and responsible, and maybe guilty or ashamed. Manipulation may involve getting someone to act or talk provocatively. Rude images or messages can be embarrassing, and fear of exposing these can make one vulnerable to further manipulation. Technology is also used to control, track and manipulate within teen relationships.

Cyberbullying– the legal context

Although bullying behaviour is not a criminal offence, there are laws that may apply to harassment or threatening behaviour, e.g. threatening and menacing communications. Some Cyberbullying could be criminal activity under a range of laws:

Protection from Harassment: This is relevant to repeated incidents. A person may be restrained from conduct amounting to harassment, and the victim may be protected.

Public Communications: Sending 'grossly offensive…obscene, indecent or menacing' communications, sending a message one knows to be false (or causing to be sent) or persistent use of a public communications system.

Malicious Communications: Sending indecent, grossly offensive or threatening communications or articles to another person with the intent to cause them distress or anxiety.

Public Order: Use of threatening, abusive, or insulting words, writing, signs etc., within the sight or hearing of a person likely to be caused; and with intent to cause; harassment, alarm or distress. This may apply where a phone is used as a camera or video.

Obscene publications: Obscene articles, published by circulating, showing, playing or projecting, or transmitting that data e.g. on a club website or intranet. Obscene articles are those whose effect could deprave or corrupt those likely to read, see or hear the matter contained or embodied.

Computer misuse: Includes hacking into a person's account, and other laws on confidentiality and privacy may apply.

Defamation: Applies to published material which damages the reputation of an individual or an organisation, and includes material published in the internet. Where material of this sort is published on a website, the person affected may inform the host and ask for removal. Once the host knows the material may be defamatory, it cannot rely on a defence of innocent dissemination.

Avoiding cyberbullying

Text/video messaging

- Do not reply to abusive of obscene messages. Your service provider should have a number for reporting abusive messages. Try their website for details.
- Do not delete the message. If abuse continues you can show messages to someone who can help.
- Be careful who you give phone numbers to and don't leave your phone lying around. Set a PIN and keep it safe.

Chatrooms / instant messaging

- Protect your personal details.
- Give yourself an alias that does not display your age, gender or location.
- Do not respond to abusive posting- ignore or log-off. If you rush to reply you may write something which may make things worse.
- Think about what you send and consider how it might be interpreted.

Email

- If you receive an abusive email do not reply. If from someone familiar, they may expect a reaction as they would if facing you directly. Do not satisfy them with a reply, and they might stop.
- If they don't stop you should trace the source of the email. Using Outlook or Outlook Express, right click over the email to reveal details of the source. You can then contact the service provider for help.
- Email may come from strangers, ('spamming'). Addresses are easy for companies to obtain and for programmes to predict. You should not reply to these, even if they have a [click to stop] link, which will confirm your address is real, and make things worse.
- You can delete these emails, but if it becomes serious you can save or print these so you have some evidence.
- Learn more about your email program from the Help menu, to find details on creating folders, filters, and routing, to help to shield you from abuse.

Internet

If cyberbullying is on a Club or community website, act as if the person displaying the bullying behaviour was face to face. Tell someone who can help. If it is on a site which is strange to you, you have to do some research to find the host of the site.

Minimising cyberbullying

Protecting personal information: Social networking can be used for both personal and rowing use so be aware of your reputation in the sport of rowing and those of colleagues. You are advised, in your own interest, to ensure that personal data is not accessible to anyone without permission to handle it. Some agencies now carry out web and social network searches to find online information about individuals – so individuals should ensure any information available is accurate and appropriate.

When publishing or messaging online – be aware of who may see the content.

What others may post about you - Use search engines to see what data is associated with your name, or your organisation. Be aware of "friending" others – i.e. giving contacts permission to view or contact you. Try to use a service that won't give contacts access to personal data, or allow collaboration without permissions.

Reporting Cyberbullying Incidents

- Employees should never personally engage with cyberbullying incidents. They should report incidents appropriately and seek support.

- Keep any records of the abuse – texts, emails, etc., and not delete. Take screen prints of web pages, and carefully record date time, and website address. Inform the person in charge at the earliest opportunity.

- Where the person initiating the bullying behaviour is known to be a current rower or co-employee, most cases will be handled best by rowing mediation and disciplinary procedures, but bullying behaviour should not be ignored and must be reported.

- Although technology seemingly allows anonymity, there are ways of tracing sources. If a potential offence has occurred, and your club cannot identify the person concerned, the police may request a service provider to disclose data about a message or its source. **Rowing Ireland** will ensure that any internal investigation does not interfere with police enquiries. Employees can of course go direct to the police

- Unfounded malicious claims may be made against others – and every claim should still be taken seriously and investigated thoroughly.

- Where an allegation is made of abuse in a way that indicates a person is unsuitable to work with children - the **Rowing Ireland Designated Children's Officer** must be informed and will be responsible for providing advice and monitoring cases. The **Rowing Ireland** Designated Children's Officer will then decide on further action.

childline

**ONLINE,
ON THE PHONE,
ANYTIME**
childline.org.uk
0800 1111

Are you being bullied?

If a young person is being bullied, they can talk to Childline anonymously online or on the phone - No worry is too big or too small.

Child Protection Online Protection: If anyone is worried about online sexual abuse or the way someone has been communicating with them online they can make a report to one of CEOP's Child Protection Advisors