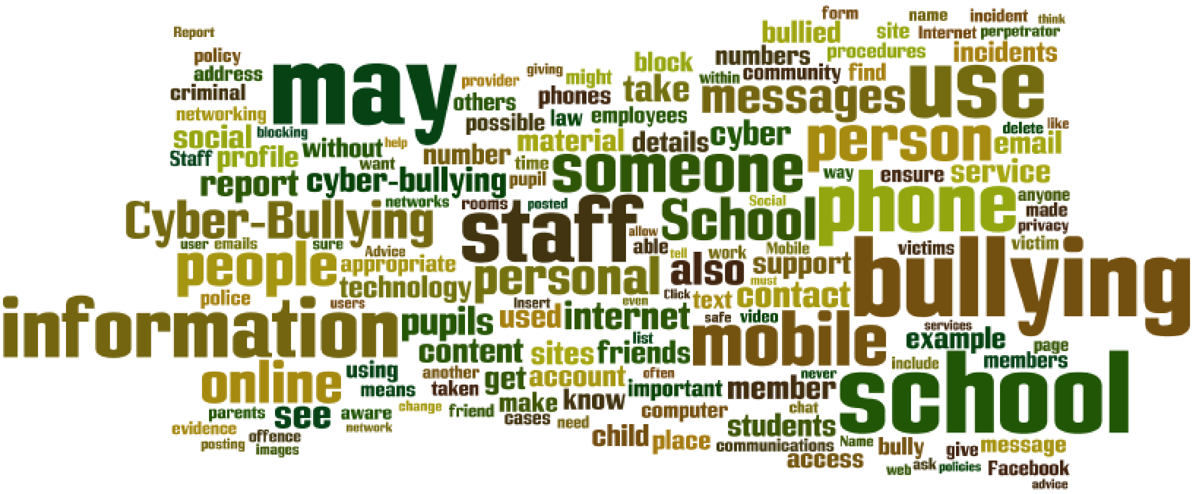
Report
policy
address
criminal
networking
social
Staff
profile
may
blocking
without
help
want
report
cyber-bullying
Cyber-Bullying
networks
people
user
emails
sure
Advice
appropriate
technology
police
users
information
online
using
means
see
parents
aware
evidence
offence
posting
images
network
provider
giving
might
others
possible
law
phones
employees
take
block
number
material
time
pupil
rooms
posted
staff
someone
details
cyber
numbers
community
messages
within
form
bullied
name
incident
think
site
Internet
perpetrator
procedures
find
use
incidents
person
email
delete
like
way
ensure
service
phone
School
Social
allow
tell
able
work
also
Mobile
must
support
victims
victim
anyone
made
privacy
bullying
personal
Click
even
text
contact
Insert
used
internet
pupils
safe
video
mobile
services
example
list
friends
sites
content
account
another
often
get
taken
change
friend
make
cases
know
need
important
computer
child
place
member
never
include
members
page
school
students
chat
communications
Name
access
bully
give
message
web
ask
policies
Facebook
advice

Contents

Some features of cyber-bullying are different to other forms of bullying:

- Cyber-bullying can take at any time and in any place. Cyber-bullying can occur in the victim's own home and while they are with friends. This can deprive victims of traditional "safe heavens".
- The audience can be very large and reached rapidly. The broad and potentially rapid reach of electronically communicated messages, coupled with potential challenges in removing them, means the scale and scope of cyber-bullying can be greater than for other forms of bullying.
- Cyber-communications can be hard to track; they may re-surface after some time. This can make it hard for victims to find closure.
- Perpetrators frequently hide behind the anonymity that electronic communications can afford them. This can mean that the traditional power imbalances (e.g. strength, perceived social status) that typify the bully-victim relationship are absent.
- In the vast majority of instances, a bully will leave some form of digital footprint that can be used as evidence (e.g. a text message, e-mail or posting on a social media site).

Cyber-Bullying and the Law

Introduction

In some cases this type of bullying can be a criminal offence. Criminal offences are investigated by the Gardaí and prosecuted by the Gardaí or the Director of Public Prosecutions. If found guilty, the person charged can face a variety of punishments including fines and imprisonment.

Contact the Gardaí if you have reasonable grounds to suspect that a criminal offence has been or is being committed. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police inquiries.

In other cases cyber-bullying can give rise to the right to bring a civil action. Civil actions are brought by the victim (or their representative). If successful, the victim might win the right to compensation, to have the offensive material removed, to an apology and/or to monetary compensation.

Criminal Law

The most relevant offences for consideration in the context of cyber-bullying are:

- assault;
- making threats to kill or cause serious injury, and;
- harassment.

A person will be guilty of the offence of assault if they, without lawful excuse, intentionally or recklessly (a) directly or indirectly apply force to or causes an impact on the body of another, or (b) cause another to believe on reasonable grounds that he or she is likely **immediately** to be subjected to any such force or impact, without the consent of the other. Force includes the application of heat, light, electric current, noise or any other form of energy, and application of matter in solid liquid or gaseous form.

This can be relevant in the context of the phenomenon of "happy slapping" where the perpetrators record an assault and then publish it online. It can also be relevant in the less common scenario in which a threat of an imminent assault was made and it was believed by the victim.

It is an offence to make a **threat** to another person, by any means intending the other to believe it will be carried out, to **kill or cause serious harm** to that other or to a third person.

In order to come within the second limb of the definition of assault, the victim must believe that they are likely to immediately be subjected to force or impact. A threat to attack someone with a hammer made to a person *via* e-mail that is sent by someone some distance away would not constitute an assault as it is unlikely to take place immediately, but it might constitute a threat to cause serious injury. No such requirement of immediacy attaches to the offence of threatening to kill or cause serious injury.

Harassment occurs when someone (without lawful authority or reasonable excuse) , by any means including by use of the telephone, harasses another by **persistently** following,

watching, pestering, besetting or communicating with him. A person harasses another where—

(a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and

(b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.

Even if the evidence is not sufficient to ground a conviction, the Court still has the power to order the accused to cease communicating with the alleged victim and/or to stay away from them if the justice of the case demands it. This allows the Court to remedy the situation where the evidence falls short of the criminal standard (beyond a shadow of a doubt) but satisfies the civil standard (the balance of probabilities).

Civil Law

In civil law, the tort of libel and the tort of slander have been replaced by the tort (legal wrong) of defamation. **Defamation** consists of the publication, by any means, of a defamatory statement concerning a person to one or more than one person. A defamatory statement is a statement that tends to injure a person's reputation in the eyes of reasonable members of society.

Data protection legislation applies to peoples details that are:

- held on a computer;
- held on paper or other manual form as part of a filing system; and
- made up of photographs or video recordings of their image or recordings of their voice.

If an organisation does not have a valid reason for holding personal details or they have taken these details in an unfair way, they can be asked to remove these details. The organisation has forty days to then remove the material, or explain why they refuse to do so. A compliant can be made to the Data Protection Commissioner if the response received is deemed inadequate or unsatisfactory. This document contains a guide to having offensive material removed and blocking unwanted telephone communications.

A Special Note on Images and Videos

Taking pictures and creating short films is easier than ever before. Employees and students can use mobile phones and webcams to capture, edit and share images. Photo and video sharing websites are extremely popular. It's important that employees and pupils are clear about their rights and responsibilities regarding taking pictures and making films.

It is important to seek permission before sharing or posting a picture of someone publicly online. Images of students should not be published online. If a picture causes distress, the subject should ask the poster to remove it in the first instance and if this does not result in the image being taken down, a request can be made to the service provider to remove the picture or film that was taken and/or posted without consent.

Consent and rights management are important topics to address with the whole-school community. The acceptable use of equipment for creating images and film (which may most typically be camera-equipped mobile phones) should be accounted for within the appropriate behaviour policy and agreements. Schools should clearly communicate expectations, acceptable conduct and potential sanctions regarding inappropriate image taking and use by staff, pupils and parents. Both pupils and employees should take care not to attach any significant personal information to publicly posted information, for example full names, without informed and/or parental consent. Even with consent, care should be taken to be mindful of basic e-safety practice.

Employment Law

Cyber-Bullying in the form of discrimination or harassment of a member of staff by another member of staff may expose the school to liability. It is the duty of every employer to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees. Incidents that are related to employment, even those taking place outside of the hours or place of work, may fall under the responsibility of the school.

Practice and Procedures

The full resources of the School community must be focused on developing and implementing policies and procedures that can effectively meet the challenge of cyber-bullying. All stakeholders must also be engaged in the school's approach to internet safety.

Members of the Board of Management, the Principle Teacher and leadership team(s) should review existing policies and procedures and identify those that must be amended to reflect the emergence of information communications technology and the widespread use of social media. This document should prove a useful guide in this endeavour.

Both staff and students may be victims of cyber-bullying and measures should be put in place to address both categories of potential victims.

Cyber-bullying can cause significant injury to the victim. Damage can be mitigated by effective and timely intervention.

Keeping good records of all Cyber-Bullying incidents and the corresponding actions by the school is essential to:

a) monitoring the and the response of the essential to monitoring the effectiveness of your school's prevention activities,
b) ensuring compliance with guidance from the Department of Education and Science
c) to review and ensure the consistency of investigations, support and sanctions.

Prevention of cyber bullying

Responding to Incidents and Reporting

Cyber bullying should be dealt with in the context of the school's countering-bullying policy. A cyber bullying incident might include features different to other forms of bullying, and may necessitate a variety of responses, depending on relevant factors:

Key factors for assessment include:

(1) Impact: possibly extensive scale and scope
(2) Location: the anytime and anywhere nature of cyber bullying
(3) Anonymity: the person being bullied might not know who the perpetrator is
(4) Motivation: the perpetrator might not realise that his/her actions are bullying
(5) Duration: how long the unacceptable behaviour went on for
(6) Coming Clean at an Early Stage and Attempting to Make Good any Damage Caused
(7) Evidence: the subject of the bullying will have evidence of what happened

School behavioural policies and procedures should explicitly refer to and outline how the school deals with Cyber-Bullying of both pupils and staff members. Cyber-Bullying incidents that are targeted at school employees should be responded to in accordance with these policies and procedures.

Staff should report all incidents to the designated manager or the Cyber-Safety Officer. The designated person will take responsibility for ensuring the person being bullied is supported,

for investigating and managing the incident, and for contacting the Gardaí and other authorities if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, friends or the Cyber-Safety Officer.

Staff should never retaliate to, i.e. personally engage with, Cyber-Bullying incidents. They should report incidents appropriately and seek support. It is vitally important to keep any records of the abuse – text, emails, voice mail, web site or instant message. Do not delete texts or emails. Take screen prints of messages or web pages, and be careful to record the time, date and address of the site.

Where the perpetrator is known to be a current pupil or co-worker, the majority of cases will be dealt with most effectively by the school's own mediation and disciplinary procedures. Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated. However, it is important to be aware that this may not necessarily lead person responsible if another person has subverted their account.

Monitoring and confiscation must be appropriate and proportionate. Parents, employees and learners should be made aware in advance of any monitoring (for example, of email or internet use) or the circumstances under which confiscation might take place.

Guidance for Staff upon Receiving an Allegation of Cyber-Bullying

If you suspect or if you are told about an alleged incidence of cyber-bullying, follow the procedure illustrated below for each method of communication:

Mobile Phones

- Ask the pupil to show you the mobile phone.
- Record the content of the inappropriate message or image. Include the date of receipt, names and phone numbers.
- Make a transcript of a spoken message.
- Tell the pupil to not to delete the communication for the moment and go with the pupil to the Principal, Cyber-Safety Office or in their absence, contact a senior member of staff.

Computers

- Ask the pupil to get up on-screen the material in question (unless the material is of a disturbing nature, in which case it may be necessary to use alternative means to locate the material such as checking the browsing history).
- Save the material to a secure location that cannot be accessed by the general population. Remember that password protecting documents does not offer the same protection as encryption.
- Print off the offending material straight away. Send it to a nearby printer to avoid the risk of interception.
- Bring the material and the paper to the Principal or, in their absence, the Cyber-Safety Officer.
- Follow the standard procedures for interviewing students and taking statements, particularly if the incident raises the issue of child protection.

Support for the Victim

The support that is required will depend upon the circumstances of the case.

Examples include:

- Emotional support and reassurance that it was right to report the incident
- Advice not to retaliate or reply, but to keep the evidence and show or give it to their parent or a member of staff
- Advice on other aspects of the code to prevent re-occurrence
- Advice on how the perpetrator might be blocked from the individual's sites or services
- Actions, where possible and appropriate, to have offending material removed
- Advice to consider changing email addresses and/or mobile phone numbers
- Discuss contacting the police in cases of suspected illegal content

Investigation

Again, the nature of any investigation will depend on the circumstances. It may include, for example,

- a review of the available evidence and advice on how to preserve it, (for example by saving or printing e.g. phone messages, texts, emails, website pages).

- efforts to identify the perpetrator, which may include looking at the media, systems and sites used. Witnesses may have useful information. Staff do not have the authority to search the contents of a phone. Where a potential criminal offence has been identified, the school should ensure that any internal investigation does not interfere with police inquiries.

Working with the perpetrator

Work with the perpetrator and any sanctions will be determined on an individual basis, in accordance with the Counter Bullying Policy, with the intention of:

- Helping the person harmed to feel safe again and be assured that the bullying will stop
- Holding the perpetrator to account, so they recognise the harm caused and do not repeat the behaviour
- Helping bullies to recognise the consequences of their actions and facilitating change in their attitude and behaviour
- Demonstrating that cyber bullying, as any other form of bullying, is unacceptable and that the school has effective ways of dealing with it

Conclusion

Cyber-Bullying can be very damaging to individuals, and disruptive to school life.

Though new technology brings incredible opportunities for educators as well as young people, it is crucial that everyone knows how to use this technology responsibly and that policies are in place to support and encourage responsible use.

School staff should be aware of what Cyber-Bullying is, and be clear about how they report it and the support in place to help them deal with incidents quickly and effectively. School leaders should ensure that measures are in place to identify, prevent and respond to Cyber-Bullying.

Evaluating the effectiveness of counter bullying procedures

The school should consider how it might most effectively measure the impact of prevention activities. Pupil, staff and parent satisfaction surveys may provide an important indication of progress. Similarly, if Cyber-Bullying activities against staff are identified, schools should review the

- effectiveness of actions taken against criteria such as:
- staff satisfaction with process and support
- effectiveness of sanction against the pupil
- effectiveness of sanctions in reinforcing school policy to other pupils.

Members of staff will report any incidents of cyber bullying to the Cyber-Safety Officer, who will review any serious incident within three months of the school dealing with it and will ensure that an annual review of cyber bullying and the counter bullying procedures is carried out

The review will take into account comments and suggested areas for improvement from staff and students, including input from the student council.

Checklist

Dealing with Cyber-Bullying is best done within a robust framework which includes and supports the whole school community.

(1) The whole-school community should be supported in gaining an understanding of what is meant by Cyber-Bullying, it's potential impact, and how it differs from other forms of bullying and why it is unacceptable.
(2) Staff should be provided with information and professional development opportunities regarding Cyber-Bullying. It is particularly important that they understand child protection and other legal issues that may relate to Cyber-Bullying incidents.
(3) Current school policy, guidance and information relevant to Cyber-Bullying should be reviewed, to ensure that it meets the needs of pupils and staff.
(4) including the use of mobile phones and cameras within school; Employee terms and conditions; Pupil and staff support and pastoral care.
(5) The whole-school community should understand reporting routes and responsibilities. A member of the senior management team should be appointed to lead on and oversee anti-Cyber-Bullying activity and incidents.
(6) Staff may find it difficult to report instances of Cyber-Bullying to their line manager, and they should feel free to seek advice from appropriate agencies outside of the school – their union or professional association, for example, or the Teacher Support Network.
(7) The positive use of technology, which models safe and effective practice, is key to preventing the misuse of technology. Schools should ensure that learning strategies and targets, as well as staff development programmes, support the innovative and engaging use of technologies.
(8) The impact of prevention and response policies and practice should be monitored annually. Staff and pupils and parents should feel confident that their school effectively supports those who are the victims of cyber-bullying.

School employees should expect:

- All incidents that they report are recorded.
- The school will respond to an incident in a timely and appropriate manner, where possible, or support the member of staff concerned to do so.
- Appropriate personal support, or information enabling them to access appropriate personal support will be provided.
- Information on the safe use of technology will be provided to them.
- The school will approach third party agencies on their behalf in order to request that inappropriate material is removed, where possible.
- The school will support the staff member in cases where it is necessary for the person being bullied to contact the service provider directly, for example where identity theft or impersonation has taken place, where an individual has a complaint about their appearance in a video, or where the incident involves contacting the staff member's mobile phone service provider.
- Where appropriate, the school will contact the Gardaí.

Where the bully is a member of the school community:

- The school will work with and take steps to change the attitude and behaviour of the bully.

- The school will take care to make an informed evaluation of the severity of the incident, taking into account the ways in which Cyber-Bullying differs from other forms of bullying.
- The school will deliver appropriate and consistent sanctions.

School employees should take steps to protect themselves and their personal information by:

- Keeping passwords secret and protecting access to their accounts.
- Not friending pupils on personal social networking services.
- Keeping personal phone numbers private and not using their own mobile phones to contact pupils or parents.
- Keeping a record of their phones unique International Mobile Equipment Identity (IMEI) number, and keeping phones secure while on school premises.
- Not posting information about them publicly that they wouldn't want employers, colleagues, pupils or parents to see.
- Ensuring that rules regarding the use of technologies are consistently enforced.
- Not personally retaliating to any incident.
- Reporting any incident to the appropriate member of staff in a timely manner.
- Keeping any evidence of an incident.