1. Understanding cyberbullying

The use of mobile and internet connected technologies are a part of everyday life. Young people and adults are socialising online, exchanging information and pictures, sharing links, and creating and uploading their own content to blogs and video hosting sites. Technology can be a powerful, positive tool, in all areas of life, including education and learning and enables us to do many things that would not otherwise be possible.

Technology does not cause people to behave badly – however, some people use technology to carry out harmful actions, including cyberbullying. It is important for school communities, and people working in educational settings that support children and young people, to understand what cyberbullying is – in order to effectively prevent and address harmful behaviour, and promote positive and constructive uses of technology.

> "We often discuss cyberbullying with our LGB&T young people, but they say the positive impact of the internet on their lives, especially when it comes to struggles they are having relating to their identities, outweighs the bad every time. I think that it is important to teach when talking about cyberbullying, as the amount of support online is invaluable for young people. Many young people I work with are told 'just turn it all off' if they talk about having problems online. We should never give this advice."
>
> Local authority e-safety peer ambassador

Addressing all forms of bullying is vital to support the health and wellbeing of members of the school community. Research shows that bullying has a significant impact on the outcomes of children and young people. Cyberbullying, like other forms of bullying, affects self-esteem/self-confidence and can have a detrimental effect on mental health and wellbeing, in the worst cases leading to self-harm and suicide.

1.1 What is cyberbullying?

Bullying is purposeful, repeated behaviour designed to cause physical and emotional distress. Cyberbullying (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks.

Cyberbullying is the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else.

- Technology can be used to carry out a wide range of unacceptable or illegal behaviours. Cyberbullying can include:

  – intimidation and threats

  – harassment and stalking

  – vilification/defamation

  – exclusion or peer rejection

  – impersonation

  – unauthorised publication of personal information or images

  – manipulation

- Cyberbullying can be an extension of face-to-face bullying, with technology providing an additional route to harass an individual or group.

- Cyberbullying can be a way for someone being bullied face-to-face to retaliate.

- Cyberbullying can be carried out by individuals or groups who are known to the person being bullied.

- There are also cases where individuals have been cyberbullied by people or groups they have never met.

- Any member of the school community – pupil, staff member, parent or carer – can be involved in and be affected by cyberbullying. Cyberbullying can take place between pupils; between pupils and staff; between parents and carers and pupils; between parents and carers and staff; and between staff members.

- Schools and other educational providers must work with the whole school community to understand, prevent and respond to bullying behaviour, including cyberbullying.

- Cyberbullying can include discrimination and hate crimes, including:

– sexist bullying

– racist and faith targeted bullying

– bullying related to sexual orientation (homophobic or biphobic bullying)

– bullying related to gender identity (transphobic bullying)

– bullying of people because they have special educational needs and disabilities

Isn't it just Free Speech?

"Abuse is different to people expressing an honest opinion which might differ to those of other people. Abuse aims to hurt. Abusers often hide behind the idea that all they are doing is expressing an opinion or a belief, but if the content or manner of the communication is threatening or intends to cause distress, then it may be against the law."

For more information see **Stop Online Abuse**.

1.2 Forms that cyberbullying can take

Threats and intimidation

- Threats can be sent by mobile phone, email, within online games, via comments on websites, social networking sites or message boards.

- Threats can include violence, including sexual violence, or threats to disclose information about someone that may harm them, or that they are not ready to share – for example, the threat to make someone's sexual orientation or gender identity known (to 'out' someone) when they may not feel ready for this.

Harassment or stalking

- Repeatedly sending unwanted text or instant messages, or making phone calls (including silent calls).

- Using public forums, such as social networking sites or message boards, to repeatedly harass, or to post derogatory or defamatory statements.

- Tracking someone's activity and collecting information about them, for example by searching databases and social network services; by pretending to be other people and 'friending' the person; or by using spyware.

- Doxing (which comes from the slang 'dox' for 'documents') is the practice of posting personal information about someone online without their permission.

Vilification/defamation

- Posting upsetting or defamatory remarks about an individual online, or name-calling, general insults, and prejudice-based bullying, for example sexist, homophobic and racist messages.

- 'Slut-shaming' can be defined as the practice of attacking (primarily) girls and women on the grounds of perceived or fabricated transgressions of socially acceptable sexual behaviours i.e. reposting of texts or images, or the fabrication of information. This practice attacks girls and women on the grounds of their gender and sexual identities, and aims to regulate their behaviour by sending the message that what is deemed as sexually inappropriate conduct can be legitimately used to publically humiliate them, whether they engage in it or not.

Ostracising/peer rejection/exclusion

- Online exclusion may be harder to detect than people being marginalised in a physical space, such as a classroom. Social networking sites can be an important extension of a person's social space and activity.

- On some services, it is possible for members to set up a closed group, which can protect members from unwanted contact, but can also be used to exclude others. Functions that can be used to block abusive behaviour can also be used to exclude others online.

Identity theft/unauthorised access and impersonation

- 'Hacking' is generally used to mean accessing someone else's account, by finding out or guessing their username and password information for example. Unauthorised access of systems, accounts or files is not automatically a form of cyberbullying, but it is always a serious issue. Unauthorised access to computer material is illegal.

- There are cases where sites have been set up which make use of school logos and name, or using photographs of staff or students taken from the school website without permission.

Publicly posting, sending or forwarding personal or private information or images

- The deliberate public sharing of private content can be designed to embarrass or humiliate, and once such messages or content are made public, containing them becomes very difficult.

- Creating, possessing, copying or distributing images of children and young people under the age of 18 which are of an indecent or sexual nature is illegal, even if they were taken in 'fun' or by 'willing' parties, or if they were taken and distributed by the subject of the photograph.

- Sharing private, sexually provocative or sexually explicit photographs or films of adults (of people aged 18 and over) without their consent, and with intent to cause distress ('revenge porn'), is an offence, regardless of whether the subject initially consented to the creation of the content or created the pictures themselves.

1.3 Characteristics of cyberbullying

All forms of bullying are harmful and unacceptable, including cyberbullying. The use of technology in cyberbullying means that there are some significant characteristics that differ from bullying that takes place in physical spaces. These include:

Profile: people do not have to be physically stronger, older, or more popular than the person they are bullying online.

Location: cyberbullying is not confined to a physical location and it can take place at any time. Incidents can take place in their own home, intruding into spaces that have previously been regarded as safe and private.

Audience: online content can be hard to remove, and can be re-circulated and reposted. The potential numbers of people who can see content posted online is very large. Single incidents of online abuse can quickly escalate into cyberbullying, for example, by reposting, sharing and comments.

Anonymity: the person being bullied will not always know the identity of the person or people bullying them. They also will not know who has seen the abusive content.

Motivation: cyberbullying is typically carried out on purpose. However, initial incidents may have unintended consequences, and can escalate through the involvement of others. An individual may not feel that by endorsing or reposting someone else's post that they are actively participating in bullying. The instigator may not have intended an offensive or hurtful comment to be repeated. A single incident – one upsetting post or message – may escalate into cyberbullying involving a number of people over time.

Evidence: online and mobile communications leave a digital trail.

Research into cyberbullying

How common is cyberbullying?

There has been a range of research in this area. Research does indicate that cyberbullying incidents are increasing, affecting children, young people, and school staff.

- **Incidents of bullying overall for children and young people in the UK have not decreased since 2010**. Face-to-face bullying has decreased, while cyberbullying has increased from 8% in 2010 to 12% in 2013. 12% of 9-16 year olds reported experiencing cyberbullying, and 9% reported face-to-face bullying.

- In other research, just over **1 in 10 (11%) young people in England said they had experienced cyberbullying by phone or online in the last year**.

Who is cyberbullied?

Cyberbullying can affect all members of the school community. However, some of the research in this area indicates that some members of the community are disproportionately affected. **Girls**, **learners with special education needs** and disabilities, and **learners identifying as gay, lesbian, bisexual** or **transgender** are disproportionately affected by cyberbullying. Cyberbullying may relate to **race, ethnicity or national origin, and religion and faith**. **All learners should feel safe and a part of their school community**.

What are the impacts of being bullied?

- Bullying can have a profound and **negative affect on the person being bullied, the person carrying out the bullying**, and on people witnessing the bullying (bystanders). Being a target of bullying **increases the risk of being depressed** later in life by more than half. Being a bully also **increases the risk of becoming depressed**.

- Bullying has been related to negative long-term physical as well as mental health impacts, and to social and economic outcomes. The effects of childhood bullying can be **evident many years later**.

Why do people cyberbully?

Reasons may include:

- personal, social or family issues

- early childhood experience, including parenting and maltreatment

- they do not like a person

- they feel provoked

- they are taking revenge or may have been bullied themselves

- an acute need for attention

- poor self-esteem, depression or anger that they cannot manage

- asserting and increasing their popularity and social status

- inability or unwillingness to empathise with others

- to feel powerful and in control

- from boredom or as a form of entertainment

While technology does not cause bullying, it may be used by people who would not necessarily bully others face-to-face. The perceived anonymity of some online activities, or disinhibition due to the physical and emotional distance between people using technology, may mean that the person bullying will do things that they would not do in person.

Bullying may also be, or felt to be, supported institutionally and culturally. Young people may be bullying within environments where respect for others, and treating others well, is not seen as important – or where disrespect and poor treatment is tolerated or encouraged. Individuals who do not conform to social norms may face discrimination within intolerant communities.

1.4 Legal duties and powers

Education settings

- All education settings have a **duty to protect students** from all forms of bullying behaviour and provide a safe, healthy environment.

- Schools are required to **ensure children are taught about online safety** though teaching and learning opportunities.

- All employers including employers of school staff have a duty to ensure the health, safety and welfare of employees.

- All school staff have a responsibility to provide a **safe environment in which children can learn**, this includes in digital as well as physical spaces.

- **Teachers**, including **headteachers**, must safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties.

- Schools have a duty to review and develop online safety as part of their safeguarding responsibilities. In England the Common Framework inspections carried out by **Ofsted** include discussions with learners relating to online safety and bullying including cyberbullying, and a review of how the school promotes positive behaviour, addresses prevention and responds to incidents.

Civil and criminal law

Bullying, or cyberbullying, is not a specific criminal offence in UK law, however harassment, malicious communications, stalking, threatening violence, and incitement are all crimes. There are a range of laws that criminalise activity that may be related to cyberbullying, including discrimination, harassment and threats.

The age of criminal responsibility in England and Wales is 10. It is worth noting the Crown Prosecution Service (CPS) **Guidelines on prosecuting cases involving communications sent via social media**:

"The age and maturity of suspects should be given significant weight, particularly if they are under the age of 18 […] Children may not appreciate the potential harm and seriousness of their communications and a prosecution is rarely likely to be in the public interest".

These laws include:

- **Equality Act 2010**: establishes that it is against the law to discriminate against anyone because of protected characteristics. Protected characteristics include disability, gender reassignment (when a person undergoes a process, or part of a process – social or medical – for the purpose of reassigning their sex), race (including colour, nationality, ethnic or national origin), religion or belief, sex and sexual orientation.

- **Protection from Harassment Act 1997**: includes criminal and civil provision for harassment (incidents that have happened repeatedly, i.e. on more than two occasions). It also provides a more serious offence of someone causing another person to fear, on at least two occasions, that violence will be used against them. Stalking, including cyberstalking, is covered.

- **Communications Act 2003**: covers all forms of improper public communications, and makes an offence of sending grossly offensive, obscene, indecent or menacing messages, or of sending (or causing to be sent) messages causing annoyance, inconvenience or needless anxiety.

- **Computer Misuse Act 1990**: may apply when cyberbullying takes the form of hacking into someone else's account. There are also additional civil laws on confidentiality and privacy.

- **Criminal Justice and Courts Act 2015**: criminalises the sharing of private, sexual photographs or films ('revenge porn') of adults without their consent, with the intent to cause distress.

- **Protection of Children Act 1978**: criminalises the taking, creating, showing, distributing, possessing with a view to distributing, and publishing any advertisement of indecent photographs of children (people under the age of 18).

- **Criminal Justice Act 1988**: makes the possession of indecent photographs of children (under 18) a criminal offence.

Understanding cyberbullying: checklist

✔ Are school staff aware of the different forms that cyberbullying can take, and the specific characteristics of cyberbullying?

✔ Does the school share a clear understanding of what cyberbullying is, and why it is not acceptable?

✔ Does the school support all staff in their duty to understand, prevent and respond to cyberbullying through policy, procedures, and regular training and development opportunities?

✔ Is the school familiar with the key laws and statutory guidance which relate to cyberbullying?

✔ Does the school effectively address the range of issues relating to bias and prejudice?

Resources

Department for Education (2016) **Keeping children safe in education: Statutory guidance for schools and colleges**

Gov.UK **Bullying at school: the law**

Department for Education (2014) **Cyber bullying: advice for headteachers and school staff**

Department for Education (2015) **Behaviour and discipline in schools**

Ofsted (2015) **Inspecting safeguarding in early years, education and skills from September 2015**

Department for Education (2015) **Working together to safeguard children**