Childnet International

CYBERBULLYING: UNDERSTAND, PREVENT AND RESPOND

Guidance for schools

Contents

Foreword 3

Acknowledgements 4

Executive summary 5

1. Understanding cyberbullying 7

- What is cyberbullying? 7
- Forms that cyberbullying can take 8
- Characteristics of cyberbullying 9
- Research into cyberbullying 9
- Legal duties and powers 10
- Checklist 11

2. Preventing cyberbullying 12

- A whole school community approach 12
- Understanding and talking about cyberbullying 13
- Updating existing policies and practices 14
- Making reporting cyberbullying easier 14
- Promoting the positive use of technology 15
- Evaluating the impact of prevention activities 16
- Checklist 16

3. Responding to cyberbullying 18

- Responding to incidents 18
- When and how to contact the service providers 19
- Investigation 21
- Changing bullying behaviour 24
- Checklist 25

4. Cyberbullying: Supporting school staff 27

- What is cyberbullying? 27
- How common is cyberbullying against school employees? 27
- Cyberbullying and the law 28
- Additional support 28
- Images and video 28
- Personal mobile devices 28
- Protecting personal information 29

5. What young people have told us 30

> "When we were younger we learned lots about cyberbullying. You have to talk about it to each generation though."
> Young person aged 16, Childnet focus group

Brought to you by: Childnet International

As part of: UK Safer Internet Centre

Supported by: Department for Education

Co-financed by the European Union
Connecting Europe Facility

Co-funded by: Government Equalities Office

Foreword

Childnet originally produced the hugely popular Guidance for schools on preventing and responding to cyberbullying in 2007 – one of the first national level resources of its kind. This was followed by guidance produced specifically for school staff in 2009. These initial guidance documents and resources have been used by schools and organisations across the UK and internationally to help effectively understand, prevent and respond to cyberbullying.

Since then, our knowledge and understanding of cyberbullying (also known as online bullying) has grown, alongside a rising demand from schools and other organisations that work with children and young people for support and information. The kinds of technologies we use have changed, and our use of technology has increased. The vast majority of people in the UK now use technology routinely to carry out a wide range of everyday activities. Digital literacy has continued to become increasingly important for children, young people, and adults alike. New research into who is being cyberbullied, and the impacts of cyberbullying, has been carried out. Although there is still more to do in this area, an increasingly complex picture is emerging of bullying behaviour that is carried out using technologies. Research also shows that cyberbullying is increasing, particularly among girls, and it is one of the most significant technology-related concerns schools and parents have.

The majority of people who spend time online have not experienced cyberbullying. However, bullying in any context can have severe and long-lasting negative effects, so it is critical that schools are equipped to help make sure that the experience of technology is a positive, productive and creative one for everyone in their community.

This new guidance has drawn from best practice and knowledge from schools, key organisations and experts working in the area, and from young people themselves.

In order to effectively respond to the challenge of bullying, schools and other providers who support young people need to ensure they understand cyberbullying, and know how to prevent and respond to incidents. Childnet International has worked with the Government Equalities Office to produce this guidance. The guidance provides important information and clear advice on the subject, and will support schools in reviewing how they take action.

Will Gardner
CEO Childnet International
Director of the UK Safer Internet Centre

Acknowledgements

This guidance was developed on behalf of the Government Equalities Office by Childnet International / Josie Fraser and in consultation with the Cyberbullying Advisory Board. Representatives from the following organisations are members of the Board and have contributed to the development of the guidance:

Anti-Bullying Alliance (ABA)

Association of School and College Leaders (ASCL)

The Boarding Schools' Association

Child Exploitation and Online Protection Centre (CEOP), a National Crime Agency Command

Children's Commissioner for England

Department for Education

The Diana Award

E-safety Ltd

Facebook

Google

Government Equalities Office

Kent County Council

National Association of Headteachers (NAHT)

NASUWT, The Teachers' Union

National Union of Teachers (NUT)

NSPCC

O2

Ofsted

Parent Zone

Professionals Online Safety Helpline

South West Grid for Learning

Stonewall

Teacher Development Trust

Twitter

The UK Safer Internet Centre

Welsh Government: Llywodraeth Cymru

YoungMinds

145 schools and organisations supporting schools (including local authorities, police forces, and advisory services) provided us with information about effective and innovative practice in relation to addressing cyberbullying.

The guidance was also developed in consultation with young people, recognising the importance of listening to their experiences and ensuring these inform the recommendations made to schools. Young peoples' opinions, concerns and understanding of cyberbullying shaped development of this guidance, and an overview of what they told us is included ('**What young people have told us**'). Childnet staff talked to five groups of young people between the ages of 12-17 in 2015 from the following schools and organisations:

\ **Holloway School, Islington, London**

\ **John Roan School, Greenwich, London**

\ **First Out group for young people, Leicester Lesbian Gay, Bisexual and Transgender Centre**

\ **Stretford High School, Trafford, Manchester**

Our sincere thanks go to the many individuals and organisations who contributed to the development of this guidance.

Executive Summary

Understanding cyberbullying

- Cyberbullying, or online bullying, can be defined as **the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else**.
- Cyberbullying is often linked to discrimination, including on the basis of gender, race, faith, sexual orientation, gender identity or special educational needs and disabilities. For example, girls report experiencing a higher incidence of cyberbullying than boys, and lesbian, gay, bisexual and transgender people are more likely to experience bullying, including cyberbullying.
- Cyberbullying, like other forms of bullying, affects self-esteem and self-confidence and can affect mental health and wellbeing, in the worst cases leading to self-harm and suicide. Addressing all forms of bullying and discrimination is vital to support the health and wellbeing of all members of the school community.
- Cyberbullying takes different forms: threats and intimidation; harassment or stalking (e.g. repeatedly sending unwanted texts or instant messages); vilification and defamation; ostracism and peer rejection; impersonation; and forwarding or publically posting private information or images.
- Cyberbullying can be characterised in several specific ways that differ from face-to-face bullying. These include the profile of the person carrying out the bullying; the location of online bullying; the potential audience; the perceived anonymity of the person cyberbullying; motivation of the person cyberbullying; and the digital evidence of cyberbullying.
- For the majority of people, most experiences of technology are useful and positive. Research figures vary but indicate that around **10% of young people** have experienced cyberbullying. Cyberbullying can affect and involve all members of the school community – pupils, staff, parents and carers.
- Every school must have measures in place to prevent all forms of bullying, including cyberbullying.
- School governing bodies and proprietors are required to ensure children are taught about online safety though teaching and learning opportunities.
- There is not a criminal offence called cyberbullying. However, there are criminal laws that apply to a range of behaviours linked to cyberbullying including stalking, threats, accessing computer systems without permission, and circulating sexual images.

Preventing cyberbullying

- A member of the senior leadership team should take overall responsibility for the school's work. The whole school community will need to be involved in prevention activities.
- Safeguarding and promoting the welfare of children is everyone's responsibility. All school staff are required to undertake regularly updated safeguarding and child protection training, which includes understanding, preventing and responding to cyberbullying.
- The key elements of an effective approach are: understanding and talking about cyberbullying; integrating cyberbullying prevention into relevant policies and practices; ensuring reporting routes are accessible and visible; promoting the positive use of technology; and evaluating the impact of prevention activities.
- Awareness-raising and promoting understanding about cyberbullying are essential to enable ongoing discussion and to ensure members of the community are not unknowingly facilitating cyberbullying because of a lack of understanding.
- Prevention activities can include staff development and home-school events such as special assemblies with parents and carers. Schools should consider creative approaches which are relevant to the technologies their community use.
- Cyberbullying can be addressed within the curriculum, for example through citizenship and PSHE, and in relation to Spiritual, Moral, Social and Cultural development (SMSC). Other curriculum areas, including drama and computing, can also help bring cyberbullying issues to life.

- Make reporting incidents as easy as possible. Provide and publicise a range of reporting routes, including anonymous routes. Bystanders should be encouraged to take an active role in prevention by reporting any incident they witness.
- Digital literacy and e-safety are important for both pupils and staff. Staff should be confident to model the responsible and positive use of technology, and to respond to incidents of cyberbullying appropriately, including incidents linked to discrimination.
- Evaluate the effectiveness of cyberbullying prevention activities. Keep cyberbullying a live issue and celebrate your successes. Share effective practice with other schools and learning communities.

Responding to cyberbullying

- The school should act as soon as an incident has been reported or identified. This will include providing appropriate support for the person who has been cyberbullied; stopping the incident from spreading and assist in removing material from circulation; and working with the person who has carried out the bullying to ensure that it does not happen again.
- The person being bullied may have evidence of the activity and should be encouraged to keep this to assist any investigation. Cyberbullying can also be reported to the provider of the service where it has taken place.
- Provide information to staff and students on steps they can take to protect themselves online – for example, advise those targeted not to retaliate or reply; provide advice on blocking or removing people from contact lists; and ask them to think carefully about what private information they may have in the public domain.
- Some cyberbullying content and activity is illegal. This includes indecent images of children (under the age of 18, including self-created images); obscene content (for example depictions of rape or torture); hate crimes and incidents, including racist and homophobic material; revenge pornography (sexual images of people over the age of 18 that have been published or forwarded without permission); threats of violence, rape or death threats; and stalking and harassment.
- If the school believes that the content or activity is illegal, or is not sure, the local police will be able to assist. In addition, the Professionals Online Safety Helpline is a free service which can provide schools with advice and signposting in relation to any cyberbullying concerns they may have – telephone: 0844 318 4772 website: **www.saferinternet.org.uk/about/helpline**
- The school should try to contain any incident as quickly as possible. Options here include contacting the service provider (or supporting the young person to contact the service provider), confiscating devices, requesting that students delete locally-held content and content posted online (where these contravene school behavioural policies).
- Schools have specific powers in relation to searching and confiscating digital devices that belong to students, and to deleting digital content. Schools should take care when exercising these powers that they do so proportionately and lawfully. Learners, parents and carers should be aware of the school's policies in relation to this.
- If the person who has carried out the cyberbullying is not initially known, steps can be taken to identify the person responsible. These can include looking at the school system and computer logs; identifying and interviewing possible witnesses; and, with police involvement, obtaining user information from the internet service provider.
- Once the person responsible for the cyberbullying has been identified, it is important that, as in other cases of bullying, sanctions are applied. Steps should be taken to change the attitude and behaviour of the bully, as well as ensuring access to any help that they may need.

What young people told us

The young people who talked to us identified a range of ways that cyberbullying could be carried out, including:

- posting comments, messages, photos or screenshots that are mean, threatening, untrue, personal, secret or embarrassing.
- anonymous messages or abuse (on social networks or online gaming).
- filming you or taking photos of you without your consent.
- 'indirect' messages when you don't directly name someone but everyone knows who you are talking about.
- fake accounts or profiles.
- excluding people from online conversations or talking behind your back.

Young people also mentioned cyberbullying could be targeted on the grounds of gender, gender identity, sexual orientation, and race.

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**

2. Preventing cyberbullying

Effectively addressing cyberbullying means making sure everyone in the school knows that bullying, including cyberbullying, is not acceptable and knows how to identify and take action against cyberbullying.

- Schools and other educational settings should take proactive measures to help prevent cyberbullying from occurring, and to reduce the impact of any incidents that do happen.
- All state schools are **required to have a clear policy** on tackling all forms of bullying, which is owned, understood and implemented by the whole school community.
- All schools are required to follow anti-discrimination laws, and staff must act to prevent discrimination, harassment and victimisation within the school.

Cyberbullying prevention should build on these requirements, promoting and maintaining a safe and welcoming environment.

Effectively addressing cyberbullying is an ongoing commitment, as a whole school community, to:

- understand and talk about cyberbullying
- keep policies and practices up to date
- make reporting easier
- promote the positive uses of technology
- evaluate the impact of your activities

2.1 A whole school community approach

For schools, 'whole school community' means learners, teachers, support staff, parents and carers, school leaders, governors, and all the people who provide support – including teaching assistants, break and lunchtime supervisors, and extended school provision staff. The school will need to provide a range of opportunities and routes for engagement with the different members of the whole school community.

The whole school community should be involved in agreeing an accessible and meaningful definition of bullying, which includes cyberbullying, and take an active role in preventing and responding to cyberbullying. As with other issues that potentially impact on the whole school community, wherever possible and appropriate, policies and processes should be discussed, agreed and developed collectively.

A positive whole school community ethos which promotes mutual respect and trust can help reduce incidents and the impact of incidents. All members of the school community should be confident that bullying behaviours and actions will be challenged, wherever they take place.

> "We have a weekly parent bulletin where we pass on information about internet issues to parents. By having this as a regular activity we can flag problem behaviours and guidance without creating moral panics about individual issues."
> Assistant principal, secondary school

2.2 Coordinate responsibility

A member of the senior leadership team will need to take overall responsibility for the coordination and implementation of cyberbullying prevention and responding strategies.

The schools anti-cyberbullying work will need to involve:

- the Senior Management Team
- staff with responsibility for pastoral care and behaviour issues
- the designated safeguarding lead (DSL)
- the IT network manager
- students
- teacher unions / professional associations representing staff
- school governors
- parents and carers

Schools should support and encourage parents and carers to talk to children and young people about cyberbullying. This will help reduce the number of bullying and cyberbullying incidents and limit the impact of harm caused.

The school will need to identify and work with key safeguarding partners from outside agencies, for example:

- the police
- the Local Authority
- the Local Safeguarding Children Board (LSCB)
- your local Broadband Consortia (if they are providing you with IT services)

Key external organisations can provide information, guidance, and training on issues relating to specific kinds of bullying – for example gender, LGB&T and disability. They can support schools and staff in understanding different discriminatory behaviours, and equip the school to recognise and challenge them.

Share cyberbullying resources, practices and ideas with safeguarding leads from other schools and local authorities to ensure joined up and effective prevention.

2.3 Understanding and talking about cyberbullying

Developing and agreeing on a shared understanding of what cyberbullying is, and supporting school-wide discussion around the issue of cyberbullying provides a firm foundation for prevention activities. Everyone should be aware of the forms that cyberbullying can take, and the characteristics of cyberbullying.

The school should consider what it could do to actively promote the welfare of groups that are disproportionately affected by cyberbullying. Include discussion of prejudice-related bullying and hate incidents. Sexist, racist, homophobic, biphobic and transphobic cyberbullying, as well as cyberbullying related to disability, should be addressed.

Many schools have found taking a creative approach to understanding and talking about cyberbullying can be particularly effective – with pupils producing plays, films, songs, websites, games and posters.

Children and young people need to be encouraged to take responsibility for their own actions, and be equipped to know how to respond if they are cyberbullied, or if they see someone else being cyberbullied. They also need to be given assurance that they are not on their own when it comes to addressing cyberbullying – that the school will help them if they or anyone they know is being cyberbullied.

"Understanding and talking about the positives of the internet can help young people who have had a tough time with cyberbullying. Social media doesn't cause cyberbullying, but services like Instagram, Facebook and YouTube can be misused. Helping children and young people support and educate each other about the impact and consequences of bullying online can be a really effective way of combatting cyberbullying."

Local Authority e-safety peer ambassador

Curriculum opportunities

In England, the Computing Programmes of Study for primary and secondary schools includes internet safety requirements at all key stages, to ensure children and young people can use technology safely and respectfully, and that they are able to identify risks and report concerns.

Schools are under a statutory duty to promote the Spiritual, Moral, Social and Cultural development (SMSC) of their pupils. This includes issues relevant to cyberbullying, including:

- developing self-knowledge and self-esteem
- understanding the difference between right and wrong
- taking responsibility for your own behaviour and making a positive contribution locally and socially
- respecting cultural differences and others

Cyberbullying can also be addressed through the citizenship curriculum, through Personal Social Health and Economic education (PSHE), as well as Religious Education (RE).

Publicising Sanctions

Pupils need to be aware of the importance of safe physical and digital environments and how to behave responsibly when using technology. Pupils, parents and carers, staff and governors should all be aware of the consequences of cyberbullying. Young people and their parents and carers should be made aware of pupils' rights and responsibilities in their use of technologies, and what the sanctions are for cyberbullying and instances of online abuse. Information should be accessible to all pupils.

Staff can be disciplined, and in some cases will be prohibited from teaching, if they participate in unacceptable professional conduct. This includes sustained or serious bullying, which includes cyberbullying.

Provide information about bullying that takes place out of school

Schools have some powers in relation to out-of-school bullying, under the Education and Inspections Act 2006. Students and parents will need to know that the school can provide them with support if cyberbullying takes place out of school.

The school should publicise arrangements for dealing with issues in school holidays, including signposting parents and learners to relevant reporting routes and external support when appropriate.

2.4 Updating existing policies and practices

Cyberbullying issues will impact on a range of other policies – staff development, ICT support and infrastructure, and e-learning strategies, for example.

Schools should ensure that their anti-bullying policy and/or school behaviour policy makes reference to specific types of bullying, including cyberbullying.

> "County schools take a wide range of approaches to ensuring their anti-cyberbullying work is effective. This includes the involvement of student councils in updating policies to ensure student voice is heard – some schools have student versions of key policies to ensure they are accessible and understood."
> Local Authority e-Safety officer

Acceptable Use Policies (AUPs) are the rules that students and staff agree to follow in order to use technology in school. AUPs represent how everyone in the school makes use of technology – what behaviour is expected and looks like within the community, to keep pupils and staff safe, and ensure the school is not brought into disrepute. Engage young people and staff in the development and drafting of AUP policies. It is important to ensure the language used is appropriate and accessible to the age or group of students it is intended for.

> "Our e-safety group has also just created a child-friendly AUP which we are about to launch. The policy has been written with input from children, staff and governors."
> Deputy Headteacher, primary school

It is for schools to decide if they wish to ban or restrict the use of mobile phones or devices or certain internet sites during school hours. It is open for schools to include in their behaviour / anti-bullying policies measures to restrict the use of mobile devices and websites as well as sanctions for their misuse. It is important that rules are well-publicised and that parents are made aware of them. All staff members should apply rules consistently.

2.5 Making reporting cyberbullying easier

Reporting any incident of bullying can be difficult for the person being bullied and for bystanders. It may be particularly difficult for young people to report cyberbullying if reporting will reveal something about their online activities that they do not want to share.

Engagement with technology involves feelings as well as actions – above all it is a social activity that allows young people to feel connected to their peers. Telling a young person who has been cyberbullied to keep their mobile phone switched off, delete an account, or to stay off the internet as a response to cyberbullying may be interpreted as a disruption of their social life and perceived as a punishment. In some cases, the knowledge that this is likely to be a response may prevent reporting.

All members of the community should recognise that asking for help is not a failing or a weakness, but a strength which shows courage and good judgement. All members of school staff should treat all disclosures of harm with respect and seriousness.

Publicise reporting routes

Make reporting incidents as easy as possible, providing a range of ways to report, including confidential and anonymous reporting routes.

All members of the community should know who they can talk to if they become aware of or suspect cyberbullying is taking place, or if they themselves experience cyberbullying. All staff should be clearly informed of reporting procedures by school leaders, and be aware how important it is to report cases as early as possible.

A bystander is someone who sees or knows about bullying or other forms of violence that is happening to someone else. Schools should ensure the community is aware of the importance of reporting all incidents they are aware of.

Setting up a pupil cyberbullying taskforce or peer support programme, or focusing on cyberbullying within existing groups – such as the school student council or student digital leaders group – can be an effective way to raise awareness and engage learners. Some organisations offer online safety peer education programmes to schools, for example, Childnet International's **Digital Leaders Programme**.

2.6 Promoting the positive use of technology

New technologies are being developed all the time. Keeping up-to-date and informed about young people's use of technologies, and their potential abuse and risks, is important. While children and young people are experts on their own use and can be a valuable source of information about technology, they may not necessarily understand all of the risks involved and the strategies for keeping their experience of technology safe and enjoyable.

Schools are required to ensure appropriate filters and appropriate monitoring systems are in place. Filtering and monitoring systems should protect learners from harmful materials, but not prevent schools from effectively teaching about and addressing online safety and cyberbullying. The UK Safer Internet Centre provide **advice on appropriate systems**.

Inflexible blocking and filtering policies can make it difficult for school staff to address incidents (for example, contacting service providers), and may restrict access to sites and information that is useful and relevant to students. Education and discussion around digital literacy, responsible use and online safety is essential to help children and young people deal confidently with problems that may arise, whether in or out of school.

It is important that learners and staff members are aware of what monitoring procedures are in place. Schools should ensure data protection procedures are adhered to in relation to monitoring data access and handling. Monitoring should be compliant with legal requirements and help protect the community against harassment, while respecting the rights of those who are being monitored.

Many schools make use of text, email, blogs and social networking services to inform and engage parents and carers. Schools should ensure staff making official use of social networking services and social media sites understand how to manage accounts responsibly.

> "We regularly post anti-cyberbullying tips and information for parents from one of our school Twitter accounts, and through an online newsletter and by letter."
> e-Safety Coordinator, secondary school

Promote online safety and digital literacy

Technology is being used in schools to support engaging, positive and effective learning, and for differentiation. Embedding appropriate technologies within practice can be used to enhance educational opportunities for all – making learning more flexible, creative, accessible and effective. Staff development around digital literacy and e-learning provides a great opportunity for staff to both develop their own practice and skills creatively, and to support children and young people in their safe and responsible use of technology.

Some young people will have restricted internet access, or restricted access to online spaces and communities, and may depend on school networks to find information, build positive connections, and participate in everyday life online in the same way their peers do. It is important that school staff do not make assumptions about young people's confidence and competence in relation to the use of technology, but support all learners in becoming digitally literate.

Some steps to take include:

- staff and students should never reply to upsetting messages or images. Instead, they should keep any evidence and report the incident.
- encourage staff and pupils to become familiar and confident with the account management tools of the services they use, particularly privacy and blocking features.
- ensure that staff and students are aware of the importance of keeping passwords confidential.
- everyone should know how to properly log out of accounts and lock devices. Students and staff should never leave unlocked devices unattended.
- staff and students should protect personal devices by using a PIN number or similar, and activate timed 'lock out'.

There is a range of resources available to schools which can be used in the classroom or to support individual learners, staff members and parents. Many are highlighted on the website of the **UK Safer Internet Centre**, where you can also find information about the annual Safer Internet Day, an opportunity to raise awareness and educate on the safe and positive use of the internet.

2.7 Evaluating the impact of prevention activities

Regular reviews of the impact of cyberbullying activities are vital to reduce incidents in the long term. The school should consider how it might measure the impact of prevention activities most effectively, as well as measuring the impact of prevention activities, and how it will communicate findings to the whole school community.

When an issue is made visible and people feel safe to discuss and identify incidents – for example, sexist or homophobic cyberbullying, it is likely that the school will see the number of reports relating to those issues increase in the short term.

Many schools conduct annual student and staff cyberbullying surveys. These address how safe members of the school community feel, how comfortable they feel in reporting cyberbullying incidents, and how happy they are with the ways incidents are dealt with. It is useful also to conduct a parent and carer satisfaction survey. Asking questions about cyberbullying will provide you with an indication about awareness and the success of your prevention work.

Publicise progress, activities and impact findings to the whole school community.

Preventing cyberbullying: checklist

- Are the senior leadership team confident and up-to-date in their knowledge of understanding, preventing and responding to cyberbullying?
- How does the school ensure the whole school community is involved in anti-cyberbullying activities, including the creation of related policies?
- Do staff have an understanding of how the children and young people in the school community use technology? Is the school familiar with the devices, sites and apps the community use?
- Do all members of staff understand how to report any incident of online abuse they become aware of? How are students encouraged to report cyberbullying?
- Does the school support anonymous and confidential reporting?
- How does the school support learners who are cyberbullied out of school hours, and in school holidays?
- How is the school providing digital literacy support and opportunities for staff and students?
- How is the school monitoring and measuring the impact of its prevention work?

Resources

The Your Own Technology Survey (YOTS) is a free tool to help schools and researchers better understand the digital technology their students use out of school.

The UK Safer Internet Centre have produced a guide for education settings and filtering providers about establishing 'appropriate levels' of filtering and monitoring: **www.saferinternet.org.uk/advice-centre/teachers-and-professionals/appropriate-filtering-and-monitoring**

The South West Grid for Learning's **360 degree safe self-review tool** is free for schools to use, and can help schools take a strategic approach to their online safety work.

The **Childnet Digital Leaders Programme** helps to empower young people in both primary and secondary schools to champion digital citizenship and digital creativity within their schools and to educate their peers, parents and teachers about staying safe online.

The Diana Award Anti-Bullying Campaign empowers young people, professionals and parents to tackle all forms of bullying as Ambassadors who help to keep their peers safe online and offline.

The South West Grid for Learning (SWGfL) **e-Safety Policy Template** addresses a range of e-safety and cyberbullying issues, and includes a section on a school 'Search and Deletion Policy', as well as an Acceptable Use Policy (AUP).

London Grid for Learning School **Online Safety Policies page** provides schools with a wide range of policy resources, information and guidance, including AUP templates and model letters for parents and carers.

Kent Online Safety (e-Safety) Guidance pages host a range of documents, policies and templates, including a school e-safety policy generator and AUP policies.

True Vision is a site providing information about identifying and reporting hate crimes and incidents, including racist and homophobic material.

Discrimination: your rights from Gov.UK.

Cyberbullying and children and young people with SEN and disabilities: guidance for teachers and other professionals (2014) Anti-Bullying Alliance.

The **Childnet STAR SEN Toolkit** provides practical advice and teaching activities to help educators explore e-safety with young people with autism spectrum disorders in Key Stage 3 and 4.

Stop Online Abuse provides information for women and LGB&T people.

Stonewall provides a range of research and resources for schools, including Staying Safe Online (2014), Working with Faith Communities, and Tackling Homophobic Language in schools.

Youth Chances is an action research project working to improve the lives of lesbian, gay, bisexual, transgender and questioning (LGBTQ) young people across England.

Government Equalities Office and Department for Education (2014) Evidence review: what works in tackling homophobic, biphobic and transphobic (HBT) bullying among school-age children and young people?

3. Responding to cyberbullying

Schools will need to address all incidents of cyberbullying that are reported or identified. Bullying and cyberbullying are often linked to discrimination. Schools should be aware of this and prepared to address it appropriately. Existing policies and procedures (including anti-discrimination, behaviour, and safeguarding policies) should equip staff to deal with all forms of bullying, including cyberbullying.

3.1 Responding to incidents

Help should be provided as early as possible. As soon as cyberbullying has been reported or identified:

- provide appropriate support for the person being bullied – making sure they are not at risk of immediate harm. Involve them in decision-making as appropriate.
- consider recording incidents, including recording action taken. Schools are not required to record incidents of bullying, however, there are many benefits to properly documenting incidents – for example, it can help with investigation into reported or suspected cases, with repeat incidents, and with providing information to parents and carers.
- if the incident does not constitute a criminal offence, work with those involved to ensure upsetting material is removed from devices and services as quickly as possible.
- if the incident does constitute a criminal offence, it should be reported according to protocols. Evidence should be secured appropriately.
- inform other staff members, and parents and carers, where appropriate.
- work with the person bullying to restore relationships and make sure all pupils involved feel safe inside and outside of school. Where there is evidence of bullying behaviour, appropriate sanctions should be applied.
- pupil/s that have been bullied should feel safe and confident that there will not be a repeat incident, and that the school community has learnt from the incident.

Bullying incidents can bring the school community into disrepute. In the case of media interest, ensure staff follow the school or local authority process for talking to and managing press contact.

> "A hate account was created online branding our female students as "sluts." Concerned emails and calls flooded in from parents and students. One of the important ways in which we responded was by talking to all our learners about what they could do to protect themselves online, and to make sure that our male students understood that this kind of abuse also effects them negatively – it doesn't just have consequences for girls. Our students shared their feelings about the account and we did feel like we addressed the issue as a community."
>
> Assistant Principal, secondary school

3.2. Identifying illegal content and activity

Some instances of online abuse and cyberbullying may be illegal. Schools should have internal procedures relating to the discovery of illegal digital content on school computers, or on learner or staff devices.

In the case of illegal activity, the police will be able to assist schools and other organisations supporting children and young people to determine what content is needed for the purposes of evidence, and how best to secure this.

Illegal content and activity includes:

- indecent images of children (under the age of 18)

School staff should not view illegal images unless doing so is unavoidable or necessary. Staff should never copy or forward illegal images.

If a young person (under the age of 18) has produced or shared material consensually, without pressure or malice, it may be appropriate for the school to manage the incident directly, after they have conducted a full and robust risk assessment.

Schools should always refer incidents to the police where they:

- involve adults
- involve coercion or blackmail
- are extreme in their nature or violent
- involve a child or children under 13
- where the child is at immediate or significant risk of harm

The UK Council for Child Internet Safety (UKCCIS) provide further advice in **Sexting in schools and colleges**.

Contact the **Internet Watch Foundation** if illegal images have been posted on the internet.

Contact **CEOP** if there is any concern that a child has been coerced into produced images, or is being groomed or sexually exploited.

- obscene content, for example depictions of rape or torture. These can be reported to the **Internet Watch Foundation**.
- hate crimes and incidents, including racist material. Contact your local police. Incidents can also be reported to **True Vision**.

- 'Revenge pornography' – the publication of sexual images of an adult without their consent. Contact the **Revenge Porn Helpline**.
- stalking and harassment. Contact the emergency services if there is an imminent threat of danger, alternatively, contact the local police or the **National Stalking Helpline**.
- threats of violence, rape or death threats. Contact the emergency services if there is an imminent threat of danger. Alternatively, contact the local police.
- images or recordings of a crime, e.g.an assault on a member of the school community are not illegal, but should be passed to the police.

Sexually explicit photographs and videos of young people under the age of 18 are legally regarded as indecent images of children. They are illegal to produce, forward or show to others, or possess, regardless of whether the pictures were taken and shared with the permission of the young person they depict.

Sexual images used to bully or coerce should be reported to the police. Where appropriate, the police are able to record incidents so as to limit the long term negative impact on young people.

3.3 Containing the incident

If images or other data break the law, they should be preserved appropriately as evidence. If content is upsetting but not illegal, then steps should be taken by the school to try to contain the incident as soon as possible.

Try to stop content that has been used to cyberbully from spreading.

The quickest and most effective route to getting inappropriate material taken down from the web will be to have the person who originally posted it remove it:

- if you know who the person responsible is, explain why the material is hurtful and request they remove it.
- pupils can be asked to delete offending content from their mobile phones or other devices.
- refusal to delete material from a personal device is likely to constitute reasonable grounds for confiscation.
- if pupils refuse to delete content, a parent or carer should be contacted.
- pupils can be asked to list to whom they have forwarded information, and where it is posted.

If the person who posted the material is not known, contact the site or service hosting the material to make a report to get the content taken down. Service providers should remove material that breaches their terms and conditions.

When and how to contact service providers

Addressing cyberbullying and ensuring the people involved take responsibility for their actions is not something that can be achieved just by using technology. Many sites and services provide blocking and privacy tools, and these features can sometimes be useful in stopping unwanted or upsetting contact. For example, if a social networking service member is receiving unwanted messages from another member, blocking the account is a way of stopping messages being received from that account.

Staff, pupils, and parents and carers can contact the service provider or host (i.e. the chatroom, the social network provider, or mobile operator) to report what has happened and get advice on how to stop this happening again. The service provider may be able to block particular senders or callers (for landlines), take down materials, or even delete the accounts of those that are abusing the service.

Reporting on social media platforms: advice from the **UK Safer Internet Centre's Professionals Online Safety Helpline**:

When making a report to a social media site it is important that you identify the correct report category, to make sure the platform can review the content correctly. For example, if a page is using the name of your school and the school logo without permission, that isn't offensive or abusive in itself – so unless the content is abusive the report will be rejected. If, you report the page for the unauthorised use of your intellectual property (school name and logo), or impersonation, the report is likely to succeed. Take some time to understand the site's terms of use. One of the most common types of calls from schools to the POSH helpline are about comments parents or carers make about the members of school staff online. While what you are reading may hurt your feelings and feel personally abusive, comments may not be objectively abusive or threatening.

The UK Safer Internet Centre provides **up to date checklists** for reporting incidents and using account management tools on a range of social networking services.

NSPCC's **NetAware** site provides a wide range of up to date guides to popular sites and apps, including messaging services, chatrooms, and social networking services.

The Professionals Online Safety Helpline can provide guidance on reporting incidents and requesting material be removed. The Helpline can escalate content to service providers when valid user reports have failed to have content removed. Phone: 0844 318 4772. **helpline@saferinternet.org.uk**.

Mobile phones

Malicious, abusive or threatening calls or texts are illegal. Calls should be reported to the mobile phone company – all UK operators have a nuisance or malicious call team, who will be able to assist and advise you. You do not need to know the person responsible for making the call.

Instant Messaging (IM) and Voice over Internet Protocol (VoIP) Services

Service providers can investigate and shut down any accounts that have been misused and clearly break the law or their terms of service. The best evidence for the service provider is archived or recorded conversations, and most IM providers allow the user to record all messages. Some services, for example Snapchat, only display pictures and messages on your phone for a short time. Users can take copies of offensive posts by taking a screen shot or by using apps that have been developed to take screenshots on behalf of the user.

It is illegal to make copies of sexual images of children under the age of 18 or possess these. Copies of indecent images of children must not be printed, saved or forwarded. In this instance, the service provider can be contacted with a description of the image, time sent and account it was sent from.

Chatrooms and message boards

Most chatrooms should offer the user the option of blocking or ignoring particular users. Some services may be moderated, and the moderators will warn users posting abusive comments or take down content that breaks their terms of use. Responsible sites will provide information about the terms and conditions for using the site, and information about how abusive and illegal content can be reported. Users that abuse the service can have their account deleted.

Social networking sites

It is normally possible to block/ignore particular users on social networking sites, which should mean the user can stop receiving unwanted comments. Users can do this from within the site. If a user's account content is public, the person blocked may not be able to access that content when logged in to the service. However, they will still be able to view public content anonymously.

Some social network providers also enable users to pre-moderate any comments left on their profile, or review pictures their name is tagged with before they are visible by others. This can help a user prevent unwanted or hurtful comments or images appearing on their profile, or being returned in searches for their name. Some services allow you to disable or restrict comments, messages and who can view your content. Account holders can also usually set their profile to private, so they can select who is able to access and see their profile and activity.

It is good practice for social network providers to make reporting incidents of cyberbullying easy, and have clear, accessible and prominent reporting features. Some reporting features will be within the profiles themselves.

Social networking services will review any reports of cyberbullying or online harassment. They may issue conduct warnings and they can delete the accounts of those that have broken their rules. Service providers only have to remove content if it is illegal, or if it breaks the terms of service of the site. Social network service providers should make clear to the users what the terms and conditions are for using the service, outline what counts as inappropriate and unacceptable behaviour, and provide prominent safety information so that users know how to use the service safely and responsibly.

Computer & mobile games

Players can block people from their contacts lists. However, in many games, players will not necessarily be known to each other. Reporting abusive incidents or players will vary depending on the type of game platform. In some games, you may be able to report abusive behaviour in game, either by submitting a complaint through the main menu, or from options provided when you click on another player's avatar, or by contacting the administrator.

3.4 Investigation

Recording Incidents

Recording incidents helps evidence that reported incidents have been successfully addressed, and allows the school leadership team and governing body to track and monitor progress, and prioritise specific incidents or approaches. For example – they may wish to record any instances of bullying that are linked to discrimination – for example, sexist, racist or homophobic bullying and cyberbullying, so that they can inform whole school's strategies for dealing with these issues. Schools are not required to record incidents, but doing so supports a robust approach to monitoring and evaluating incidents.

Preserve the evidence

Schools should advise pupils and staff to try to keep a record of abusive incidents, particularly: the date and time, the content of the message(s), and where possible a sender's ID (e.g. username, email, mobile phone number) or the web address of the profile/content. Taking an accurate copy, preferably a screenshot (an image which captures what you can see on the screen) – where this is legal, or record of the web-page URL will help the service provider to locate the relevant content.

Keeping evidence will help in any investigation into the cyberbullying by the service provider, but it can also be useful in showing what has happened to those who may need to know, including parents, carers, teachers, and pastoral care staff.

Digital evidence can be captured in a range of ways:

- Save evidence by taking a copy of what appears on the screen (a screenshot). The way you do this will depend on the type of device you are using.
  - On a Windows PC, hold down the Control (ctrl) key (or Function (fn) on most laptops) and press Print Screen (print scrn/PrtScr or Prt Sc) key.
  - On a Mac, hold down the Command (cmd), and press 3.
  - Taking screenshots on a mobile phone will vary from device to device. Typically, you will need to press the power button at the same time as another button. Screenshots will be saved to your image or pictures folder.
- Mobile phone messages, whether voice, image or text, should be saved. Messages that have been forwarded, for example to a staff member's school phone, won't include all of the information from the message, like the original sender's phone number.
- Some services will delete content or messages from the account of both the person who has received the message, and the person who has sent the message, if either person deletes it (for example, direct messages (DMs) on Twitter). Some services automatically delete messages after a period of time, or once they have been viewed (for example, Snapchat)
  - You can take a screenshot to capture evidence you think might be deleted this way.
  - On a phone, Flight Mode will take the device offline. Evidence cannot be deleted remotely while it remains disconnected.
- Some Instant Messaging services allow the user to record all conversations.
  - Capture messages by switching any record/archive feature on.
  - Conversations can also be printed, or sections can be saved as a screenshot.
  - Copied and pasted conversations are less useful as evidence, as these could be edited.
- On social networking sites, video-hosting sites, or other websites, keep the site link, print page or produce a screenshot of the page and save it.
- In chatrooms, print the page or take a screenshot of the page.
- Emails can be printed or forwarded to the person investigating the incident. Save or forward all subsequent emails. Preserving the whole message, and not just the text, is more useful as this will contain information about where the message has come from.

Identifying the person carrying out cyberbullying

Although the technology seemingly allows anonymity, there are ways to find out where messages or data were posted from. However, technical investigations may not necessarily identify an individual. If another person's phone or school network account has been used, locating where the information was sent from will not by itself determine who the sender was. There have been cases of people using another individual's phone or hacking into their IM or school email account to send nasty messages.

In cases where the identity of the person carrying out cyberbullying is unknown, there are some key questions to ask:

- Was the bullying carried out on the school system? If yes, are there logs in school to see who it was? Or are there records of which student was using a particular device at the time the incident occurred? The school network manager or technical support will be able to tell you what is possible.
- Are there identifiable witnesses or friendship groups who can provide information? There may be others who have visited the offending site and left comments, or who have received copies of images.
- If the bullying was not carried out on the school system, was it carried out on a mobile, or a particular internet service or game? The service provider, when contacted, may be able to take some steps to stop the abuse by blocking the aggressor or removing content it considers defamatory or breaks their terms of service. However, the police will need to be involved to enable them to look into the data of another user (see below).
- If the bullying was via mobile phone, has the person responsible withheld their number? If so, it is important to record the date and time of the message and contact the mobile operator. Steps can be taken to trace the call, but the mobile operator can only disclose this information to the police, so police would need to be involved.
- Has a potential criminal offence been committed? If so, the police may have a duty to investigate. Police can issue a RIPA (Regulation of Investigatory Powers Act 2000) request to a service provider, enabling them to disclose the data about a message or the person sending a message. This may help to identify the person responsible. Relevant criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation (for example grooming or inappropriate sexual contact or behaviour).

> "Pupils are told that they can report bullying incidents electronically on the school learning platform. A child sent us a message about an upsetting photo that had been put online without his permission, and comments that were being made on in. The same children had been name calling him in school. After talking to the child, the teacher spoke to the other pupils involved individually. They admitted uploading the photo and adding the hurtful comments. The child who had posted the photo agreed to delete it and they all wrote an apology letter. The parents of the pupils were informed, and it was suggested they talk to their children about appropriate behaviour online. They were also invited to attend our next e-safety workshop for parents if they wanted to find out more."
>
> Assistant Headteacher, primary school

Seizing and confiscating items

Staff members can confiscate, retain or dispose of a pupil's property as a disciplinary penalty, where this is reasonable. This can include mobile phones when they are being used to cause a disturbance in class or otherwise contravene the school behaviour / anti-bullying policy. The law protects members of staff from liability in any proceedings brought against them for any loss of, or damage to, any item they have confiscated, provided they acted lawfully.

Where a device contains material that needs to be passed to the police, school staff can confiscate and secure the device, for example by placing it in a locked draw.

Where a member of staff finds an item which is banned under the school rules, i.e. evidence which relates to cyberbullying but does not constitute a criminal offence – they should take into account all relevant circumstances and use their professional judgement to decide whether to return it to its owner, retain it or dispose of it. Legal content can be deleted, but staff should be aware of how to capture and retain evidence of cyberbullying incidents and of when this would be useful.

It is recommended that where possible school staff do not delete content. Young people can be asked to delete offensive or upsetting content, and confirm they have done so.

Where text or images that contravene the school's behavioural policy or the law are visible on a device, staff should act on this. All school staff can request a pupil reveal a message or show them other content on their phone for the purpose of establishing if bullying has occurred. All school staff in England can search learner-owned devices with the consent

of the pupil. Only headteachers, and members of staff who have been formally authorised by the headteacher, can search a pupil or a pupil's device without consent. They can only do so where they have reasonable grounds for suspicion the device contains items specified as prohibited. 'Prohibited items' include pornographic images, or articles that have been or could be used to commit an offence or cause harm, or that are banned in the schools published rules.

Searches without consent can only be carried out on the school premises, or in another location in England where the staff member has lawful control or charge of the pupil (for example, a school trip in England). These powers only apply in England.

Except in cases where there is reasonable suspicion that serious harm will be caused unless the search is carried out immediately, the authorised staff member searching the pupil without consent must be the same sex as the pupil, and another staff member should be present as a witness. The power to search without consent enables the requirement of the removal of outer clothing (e.g. a coat) and the searching of pockets. Only police officers can carry out more intimate searches.

Searching electronic devices

Caution should be exercised in relation to undertaking such searches. The situations where this power may be exercised should be clearly detailed in the school's bullying or behaviour policy. It is recommended that school staff should not search through electronic devices unless this is unavoidable.

Searching, screening and confiscation (Department for Education, 2014) provides the following statutory guidance in relation to electronic devices:

"Where the person conducting the search finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The member of staff must have regard to the following guidance issued by the Secretary of State when determining what is a "good reason" for examining or erasing the contents of an electronic device:

- In determining a 'good reason' to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.
- If inappropriate material is found on the device it is up to the teacher to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.
- Teachers should also take account of any additional guidance and procedures on the retention and disposal of items that have been put in place by the school."

In the UK, privacy is protected under Article 8 of the Human Rights Act 1998. Article 8 is a qualified right, which means that if a public authority believes it is in the greater interest of the community, or to protect other people's rights, it can interfere with the right to a private life. Any breach of Article 8 should be appropriate to the balance of qualification.

Investigating allegations against staff

Some messages might allege abuse against a teacher or other member of staff. There have been cyberbullying incidents where pupils, or parents and carers have made unfounded and malicious claims against staff members. It is critical to take every claim seriously and investigate it thoroughly.

Students, staff, parents and carers should also be made aware it is an offence to publish the name of a school staff member who is subject to an allegation against a current pupil, until such a time as they are formally charged with an offence. 'Publishing' includes posting details of an allegation on a social networking site that could lead to the identification of the staff member by the public.

The school is legally required to act in cases where an allegation is made that an employee or volunteer has:

- behaved in a way that has harmed or may have harmed a child.
- possibly committed a criminal offence against or related to a child.
- behaved towards a child or children in a way that indicates s/he is unsuitable to work with children.

Regardless of where the alleged abuse took place, the allegation should be reported to the headteacher immediately. The headteacher will contact the local authority designated officer for child protection concerns. In cases where the headteacher is the subject of allegations, the Chair of Governors or equivalent will contact the designated officer.

The local authority designated officer will decide whether to consult the police or children's social care services. Detailed guidance on dealing with allegations of abuse is provided in ***Keeping children safe in education*** (Department for Education, 2015).

Schools have a duty of care to their employees. Any allegations should be reported and investigated as quickly as possible, and the staff member should be supported during the period of investigation. Staff can also seek additional advice and help from a range of organisations, including their union, professional association, and from the Teacher Support Network.

3.5 Changing bullying behaviour

Once the person/s responsible for cyberbullying have been identified, it is important that – as in other cases of bullying – appropriate sanctions are applied.

> "Cyberbullying issues are dealt with in the same way as physical bullying in school. The same sanctions are given, and any problems at home are followed through in school if they are reported to us."
> e-Learning Advisor, primary school

Individuals or groups carrying out the cyberbullying may say they are 'only joking' or that it is just 'banter' and that their behaviour has been misinterpreted. They may believe that the problem is not that they are bullying someone else, but that the person they are bullying reacts badly to their behaviour (e.g. they 'do not have a sense of humour').

The school should work with the pupil or pupils to ensure they recognise the consequences of their actions, and are supported to change their attitude, behaviour, and the way they use technology. You may want to adopt restorative approaches to change behaviour.

> "I recently supported a primary school where some Year 6 children were bullying on Instagram. The school had delivered e-safety education within PSHE and computing, so pupils knew that they should take a screenshot of any bullying and tell a trusted adult – in this case, their class teacher. I and the schools designated safeguarding lead (DSL) supported the teacher, and the incident handled in line with the school policy - treating cyberbullying like any form of bullying. One parent was initially reticent, however when they saw the screenshots of the content their child had sent, they were happy to work with the school. The school took a restorative justice approach which was felt to be successful by the children, staff and parents involved."
> Local Authority e-Safety Officer

The purpose of sanctions and the school's work with the person responsible for bullying is to:

- help the person harmed to feel safe again, and be assured that the bullying will stop.
- ensure the person carrying out the bullying takes responsibility for their actions, recognises the harm caused, and does not repeat the behaviour.
- demonstrate to the school community that cyberbullying is unacceptable and that the school will actively address all incidents.

Responding to cyberbullying: checklist

- ✔ Do pupils and staff understand the basics of keeping themselves safe online – including privacy settings, reporting, and getting material taken down?
- ✔ Are staff familiar with the school's processes for responding to cyberbullying?
- ✔ Are staff and pupils aware of the ways in which the school provides support for people who are bullied? Are people who have been bullied appropriately involved in the decision making and resolution process?
- ✔ Do pupils and staff understand which kinds of cyberbullying may be illegal? Do staff know what to do if they suspect cyberbullying activity is illegal?
- ✔ Are clear processes and policies in place in relation to searching pupils, confiscating devices and deleting materials?
- ✔ What are the consequences for bullying, including cyberbullying in your school? Is the whole school community clear about sanctions?

Resources

Searching, screening and confiscation: advice for schools (Department for Education, 2014)

Keeping children safe in education (Department for Education 2015) **Part Four: Allegations for abuse made against teachers and other staff**.

Sexting

Several organisations provide advice and guidance about sexting and youth produced sexual imagery. Making, possessing and distributing 'indecent' images of anyone under 18 is illegal, and may have negative consequences for the young people involved.

Sexting is not necessarily related to bullying, however, images or video may be used to cyberbully or manipulate people.

- UKCCIS: **Sexting in schools and colleges**

Further resources:

- CEOP ThinkUKnow: **Selfies: The naked truth**
- UK Safer Internet Centre: **sexting resources**
- Childline: **Sexting resources**

Contacting service providers

Mobile phone operators

- **EE**, (Orange and T-Mobile): Call 150 from your EE phone, or 07953 966 250 from any phone.
- Telefónica/O2: Email **malicious@telefonica.com**, or call 202 (from a Pay Monthly phone) or 4445 (from a Pay As You Go phone).
- **Tesco Mobile**: Call 445 from a Tesco Mobile phone, or 0345 3014455 from any phone.
- **Three**: Call 333 from a Three phone, or 08707 330 333 from any phone.
- **Vodafone**: Call customer services on 191 from a Vodafone phone or on any other phone call 08700700191 for Pay Monthly customers or on 08700776655 for Pay As You Go customers.

VOIP and IM Services

- **Facebook Messenger**: Information on reporting abusive messages can be found here
- **Google Hangouts**: Reporting abuse in public video hangouts in Google+
- **Kik**: Reporting abuse
- Skype: You can report abuse on Skype **here**
- Snapchat provide **safety information and reporting options**
- **Whatsapp** provide safety and security information on using the service

Email providers

- **Gmail**: Information on blocking unwanted emails, and reporting a Gmail user who is sending harassing emails
- **Yahoo! Mail**: Advice on receiving threatening emails
- **Outlook Mail** (including hotmail.com, msn.com and live.com)

Social network service providers

- **Facebook**: Facebook provide a range of information at their online *Family Safety Centre*, including a bullying prevention hub
- **Google**: Google provides a range of information about keeping yourself, your accounts and others safe at their *Online Safety Centre*, including information about reporting and safety tools
- **Instagram**: You can reporting abusive posts on the web or from the **app**. Instagram hosts an online *Help Centre* which provides **privacy and safety advice**
- Twitter: You can report abusive incidents or harassment **here**. The Twitter Safety Centre provides **information for young people, families and educators**
- YouTube: In order to report content to the site provider as inappropriate. You will need to log in to your account, or create an account if you don't already have one (this is free), and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the video content itself, and you can also flag individual comments under a video. YouTube provides information on its policies and reporting tools at its ***Policy and Safety Hub***.

Games

- **PlayStation**: Reporting abusive players will depend on the console you are using
- **Steam**: Reporting abusive behaviour in the Steam Community
- **Xbox Live**

4. Cyberbullying: Supporting School Staff

The use of technology can provide incredible opportunities for school staff, as well as young people. It is crucial that everyone knows how to use technology responsibly. School staff should:

- be aware of what cyberbullying is.
- be clear about how they report incidents.
- know what support is in place to help them deal with incidents quickly and effectively.
- be provided with opportunities to develop their digital literacy.

Cyberbullying can seriously impact on the health, wellbeing, and self-confidence of those targeted. It may have a significant impact not only on the person being bullied, but also on their home and work life too. Career progression may be affected, and there have been cases where the person bullied has chosen to leave the education sector altogether. Dealing with incidents quickly and effectively is key to minimising harm in potentially highly stressful situations.

All employers, including employers of school staff, have statutory and common law duties to look after the physical and mental health of their employees. Protecting staff from cyberbullying is best done within a prevention framework, with whole school policies and practices designed to combat cyberbullying. Each school should have a designated cyberbullying lead – a member of the senior management team who will oversee and manage the investigation and resolution of all incidents.

Staff members who are subject to cyberbullying or online abuse should:

- never personally retaliate.
- keep evidence of the incident.
- report any incident which relates to their role as a school employee to the appropriate member of staff as soon as possible.

What is cyberbullying?

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

- Cyberbullying can consist of threats, harassment, embarrassment, humiliation, defamation or impersonation.
- Cyberbullying may take the form of general insults, or prejudice-based bullying including hate crimes, for example homophobia, racism, sexism or other forms of discrimination.
- There have been cases of school employees being cyberbullied by current or ex-pupils, parents and carers, and by colleagues, as well as by people who attempt to remain anonymous.
- There are reported cases of cyberbullying involving a wide range of technologies and services, including social networking sites, apps, email, instant messaging (IM), learning environments, games and by mobile phone.

How common is cyberbullying against school employees?

School workforce unions, professional associations and industry providers have noted an increase in cyberbullying reports and related inquiries, and are committed to working to reduce incidence and support schools to deal with incidents effectively.

Cyberbullying incidents can be extremely upsetting – even devastating – for the victim, whatever age they are.

All forms of bullying, including cyberbullying, should be taken seriously. Bullying is never acceptable, and should never be tolerated.

Cyberbullying and the law

While there is not a specific criminal offence called cyberbullying, activities related to cyberbullying may be criminal offences under a range of different laws.

- Cyberbullying in the form of discrimination or harassment of a member of staff may mean that the school has breached its duties under discrimination legislation.

  Schools are liable for the actions of staff members who discriminate against or harass other staff members in the course of their employment. Schools should ensure such acts are understood by their community as unacceptable. Where schools become aware that an employee has been subjected to harassment, they will need to take steps to prevent it from recurring.

- It is the duty of every employer under health and safety legislation to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees.

  Staff resignation as a consequence of cyberbullying, in cases where the school has failed to take adequate steps to address the situation, may prompt claims of constructive dismissal.

- **Schools are required** to provide staff with training and information relating to abuse, including cyberbullying; have procedures in place for addressing cyberbullying incidents; and include acceptable use in relation to online and mobile communications in their staff behavioural policy.

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 employer.

Additional Support

Staff should be aware of alternative routes they can access for additional support. These include:

- their Union or professional association
- **The Professionals Online Safety Helpline**: 0844 381 4772 **www.saferinternet.org.uk/about/helpline**
- occupational health services
- **Education Support Partnership**: Helpline: 08000 562 561 (UK-wide)
- other helplines such as the **Samaritans**

Images and Video

Employees and learners use a wide range of devices, including tablets and mobile phones, to take photographs and videos. Photo and video-sharing websites and apps are extremely popular, and are used by schools to capture learner progress, showcase events and share presentations. Employees and pupils should be informed about their rights and responsibilities regarding taking pictures and making films.

- Photos and video taken for personal use are exempt from the **Data Protection Act** (1998), for example, a parent taking photographs of a school event.
- The Data Protection Act ensures that personal information – which includes images of staff and students where they are identifiable – is processed fairly. To do this, schools should obtain consent from each student's parent and carer, and from all students who are 12 years old or over. Consent should be obtained in advance, with an explanation of why images are being taken and what they are going to be used for – especially if they are going to be published online.
- The acceptable use of equipment for creating images and film (which may most typically be mobile phones) should be covered by the appropriate behaviour policy and agreements.
- The school can request that students and staff should not take, share or publish photographs of other members of the school community without the subject's permission. Schools should clearly communicate expectations, acceptable conduct and potential sanctions regarding inappropriate image-taking and use by staff, pupils and parents.
- School-owned devices should be provided for staff members who need to take images of pupils for school purposes.
- Both pupils and employees should take care not to attach significant personal information to publicly posted information, for example full names.

Personal Mobile Devices

School employees should secure their phones when not in use, by setting up a timed lock following a short period of inactivity, and using a pin code or password. If a phone goes missing or is suspected as being stolen, it should be reported to the police and mobile operator as soon as possible, using the phone's unique International Mobile Equipment Identity, or IMEI number. This can be found printed on the phone underneath the battery, or by typing *#06# on a handset.

If it is necessary for an employee to lend a pupil a mobile phone, staff should use a school owned device. If being able to contact pupils by their mobile becomes necessary – for example on a school trip – school employees should only use school-owned mobiles to store numbers and contact pupils. Numbers can be deleted following the event, and learners will not have access to an employee's personal number. Security features, such as a time-activated PIN or passcode, should be used to ensure that if a school-owned phone is lost or stolen, content will be inaccessible.

> "I rang a parent with my mobile over a normal school matter. My mobile number was passed around and got into the hands of some teenagers who sent abusive messages."
> A staff member

Employees should be given clear guidance regarding the use of their personal mobile phone by their employer, regarding having access to pupils' numbers, storing pupils' numbers, and giving pupils access to their personal numbers.

Protecting personal information

Many school employees use web-based and social networking services for both personal and work related purposes. Some people will choose to restrict their connections to people that they know well. Many staff use online services and sites to connect to new people – for example, in order to share work and develop professional networks.

- While school employees are private individuals, they have professional reputations and careers to maintain.

  The Teachers' Standards outline the legal minimum requirements for teachers practice and conduct. Teachers, including headteachers, should safeguard children's wellbeing and maintain public trust in the teaching profession as part of their professional duties.

- School staff should be supported in their use of technologies including social media.

  Schools are required to ensure staff receive regular training and information relating to online safety and cyberbullying. In addition, school staff behavioural policies must include the acceptable use of technologies and the use of social media, including communications between staff and students.

  For further information about these requirements, see the Department for Education statutory guidance, **Keeping children safe in education**.

- Staff should take steps to ensure they protect their personal data.

  Staff should be aware that many employers carry out web and social network service searches to find online information about staff – background, interests, career experiences and self-presentation. All staff, including new staff in training and induction, need to be advised to ensure that publically available information about them is appropriate.

- Communications online are rarely private. Others may pass on or re-post material shared digitally.

  When posting information, personal contact details, video or images, ask yourself if you would feel comfortable about a current or prospective employer, colleague, pupil or parent, viewing your content.

  Make sure you understand who is allowed to view personal content on the sites that you use – and how to restrict access to your account where necessary. If you are not clear about how to restrict access to your content to certain groups of people, regard all of your content as publicly available and act accordingly.

- Do not 'friend' current or past pupils or add them to your contact lists on personal social networking accounts.

- Information sent using official school accounts or equipment will usually be accessible to the school for monitoring purposes (this will be outlined in the schools Acceptable Use Policy), and information may also be requested under the Data Protection Act.

- You can also check to see that other people aren't misrepresenting you or treating you unfairly online. If you find things you object to, you can ask the poster to take these down in the first instance.

  Where cases are work-related, these should be reported to your line manager or to the appropriate person as soon as possible. More serious incidents, including cyberbullying, will require a formal response from your employer, and will be dealt with within the schools' disciplinary frameworks, or in more serious cases, legal frameworks.

You can check to see if others are creating or posting objectionable material about you online:

- You can use search engines to check what images and text are associated with your name, or with a combination of your school and name. This will help establish what information other people can easily find about you.

- You can search within social networking services.

- Staff may only become aware of other people posting objectionable material when a colleague or student alerts them. Encouraging everyone to report any inappropriate material they find is an important way to address cyberbullying.

> "Unfortunately we have had incidents of inappropriate comments made about school staff members on social networking services. A Facebook and Twitter account was set up deliberately to attack the school and its staff. After consulting the Professional's Online Safety Helpline, we were successful in our dealings with Twitter to get the site taken down and with Facebook to remove the school's branding. We were quick to move when alerted to this content, giving strict instructions to staff not to engage with these individuals online which I am sure stopped the problem escalating."
> e-Safety Co-ordinator, secondary school

5. What young people have told us

What did young people tell us about effective approaches in preventing and responding to cyberbullying?

This guidance has been developed in consultation with young people. Childnet International talked to five groups of secondary-aged young people between the ages of 12-17, about cyberbullying, what effective strategies schools are implementing and what can be improved to help support young people more effectively.

What are young people's definitions and experiences of cyberbullying?

The young people were able to define cyberbullying in the following ways:

- posting comments, messages, photos or screenshots that are mean, threatening, untrue, personal, secret or embarrassing. Young people also mentioned cyberbullying could be targeted on the grounds of gender, gender identity, sexual orientation and race.
- anonymous messages or abuse (on social networks or online gaming).
- filming you or taking photos of you without your consent.
- 'indirect' messages when you don't directly name someone but everyone knows who you are talking about.
- fake accounts or profiles.
- excluding people from online conversations or talk behind your back.
- Young people highlighted a range of reasons why people might cyberbully others, including: boredom, acting tough, jealousy, hiding behind a screen, grudges or disagreements, wanting attention, peer pressure or those who had been bullied themselves might want others to experience what they have been through.

Young people also identified a number of experiences in relation to cyberbullying:

- cyberbullying often happens alongside offline bullying.
- a range of popular services were named where cyberbullying takes place, including social networks and online gaming platforms.
- cyberbullying doesn't always have to be extreme, but it can be the regularity or the number of people involved that makes it particularly upsetting.
- while many young people were aware of cyberbullying incidents in their school, they also recognised that they might not always know about it.
- there can be a tendency to typecast people as either a "bully" or a "victim" but it is often not as clear cut as this.

What awareness do young people have on school rules around cyberbullying?

- Some young people were very aware of rules around cyberbullying and what the consequences would be, while others knew you would get in trouble for cyberbullying but said they hadn't been explicitly told about it. Some young people didn't think there were any rules at all.
- Most young people found out about the rules around cyberbullying because they saw what happened with an incident in school; for example, a pupil being excluded. However, young people also commented on issues that went unpunished or were not reported to school in the first place.
- Some young people felt that schools often did not have rules about bullying on the grounds of sexual orientation, gender or gender identity. Young people felt they were told that cyberbullying was wrong, but not told about different types of prejudice-based bullying.

Where would young people turn if they were being cyberbullied?

- Friends or siblings.
- Parents or other family members.
- A few young people would turn to a teacher or counsellor, and often named a particular teacher who had responsibility for offering pastoral support to pupils.
- Some young people wouldn't tell anyone if they had been cyberbullied.

What reasons did young people give for why they might not tell someone they were being cyberbullied?

- Fear of the bully or worried the bullying might escalate
- Embarrassment
- Not wanting others to see them as a 'snitch'
- Telling someone would be perceived as a sign of weakness
- Feeling that people would not care
- Being threatened or blackmailed into not speaking out
- Belief that they were somehow responsible for being bullied
- Did not think adults would believe them, or understand what cyberbullying was
- Would only tell if the bullying got really bad
- Worry that parents might confiscate devices or stop them from going online

What reasons did young people give for why they might not tell a school staff member they are being cyberbullied?

- Uncertainty about who to turn to in school or teachers being too busy
- Fear of everyone at school finding out if they told a teacher
- Feeling the schools don't have a detailed enough understanding of social networks and other online services
- For LGB&T people, perception that school staff lack familiarity with issues relating to gender identity and sexual orientation
- Teachers might not feel they have a role to play as it's something that happens in a young person's private life.
- Feeling that schools don't take an interest in cyberbullying or take it seriously
- If they were being cyberbullied by someone from another school or being cyberbullied anonymously – feeling that the school would not be able to help

What would make it easier for young people to turn to someone at school?

- Having an approachable member of staff that pupils feel comfortable around and knowing what times they would be available
- More confidential and private routes for reporting concerns
- Assurance that if they reported concerns it would not result in everyone in the school finding out
- Being able to speak to someone their own age like peer mentors
- Inclusion of cyberbullying when the school talks about bullying
- Cyberbullying should not be addressed as an isolated issue, but be integrated across behavioural, pastoral and citizenship activities

What young people would do to help someone who was being cyberbullied

- Positive approaches include:

– being aware of risks and managing these ahead of time (i.e. only friending trusted people on identifiable accounts, protecting personal information and using privacy settings).
– telling a trusted adult.
– supporting the person who is being cyberbullied (i.e. making sure that they didn't feel alone, trying to cheer them up, helping them to report, giving practical advice – e.g. showing them how to use blocking and privacy settings).

- Approaches to be cautious of include:

– relying solely on support from friends or siblings.
– standing up for the person being bullied – with the risk of getting drawn into the incident.
– reacting to the incident by removing themselves from the situation or changing their behaviour (i.e. closing accounts, changing user names or using a different app).

- Risky approaches include:

– getting angry and cyberbullying the person back, or physically attacking the person doing the cyberbullying.
– doing nothing and advising others to ignore it.

www.childnet.com

Childnet International