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.