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**