Boundary Oak School

Cyberbullying Policy

2026

This is a whole school policy and applies to EYFS and Boarding.

This policy should be read in conjunction with Anti-Bullying Policy, Safeguarding Policy (including Prevent), Online Safety Policy, Acceptable Use Policy and Staff Code of Conduct.

The school recognises that a bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm.

PERSON RESPONSIBLE FOR THE LATEST REVISION	Designated Safeguarding Lead Deputy Head Pastoral
LAST REVIEW	December 2025
LAST UPDATE	December 2025
NEXT REVIEW	December 2026

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 a method of bullying and should be viewed and treated the same as "real world" bullying and can happen to any member of the school community. Educational setting staff, parents and young people must be constantly vigilant and work together to prevent and tackle bullying wherever it appears.

Cyberbullying is a method of bullying that is concerned with the use of ICT to upset, threaten or humiliate someone and should be treated as seriously as other forms of bullying. Cyberbullying rarely occurs in isolation and tends to include physical and emotional bullying offline.

- What can sometimes make cyberbullying feel harder to manage can be the following: Cyberbullying can take place 24/7, creating a feeling of "no escape" for the victim, and is not restricted by location
- Electronic content is very hard to control once it has been posted and can never be guaranteed to be removed totally from circulation; this can be very upsetting to victims as they can never be sure who has viewed images or content about them.
- Bullies can attempt to be anonymous and can feel "distanced" from the incident. They are often unaware of the laws regarding harassment, and the fact online activity can be traced via "digital footprints."
- "Bystanders" can easily become perpetrators by passing on videos, image or content, or by videoing incidents such as "happy slapping"'
- Cyberbullying can occur unintentionally, often due to a lack of awareness and empathy, or by thinking "It was only a joke."
- Cyberbullying enables harassment and upsets to take place across generations; age and size is not an issue due to technology removing the power and size issues that could otherwise prevent bullying from occurring.
- Cyberbullying can sometimes even be perpetrated by the victim themselves (known as cyber/digital self-harm).
- One key positive with online bullying is that incidents can be used as evidence - e.g. text messages, messenger conversations, screenshots. It is important that this evidence is kept, not deleted and the victim does not retaliate.

1) CYBERBULLYING AND THE LAW

Bullying is never acceptable, and the school fully recognises its duty to protect all its members and to provide a safe, healthy environment for everyone.

Education Law:

- The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to cyberbullying. Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off the school site.
- The Act also provides a defence for staff in confiscating items such as mobile phones from pupils.

Civil and Criminal Law:

- There is not a specific law which makes cyberbullying illegal but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990).

Preventing Cyberbullying

As with all forms of bullying the best way to deal with cyberbullying is to prevent it happening in the first place. There is no single solution to the problem of cyberbullying, but the school will do the following as a minimum to impose a comprehensive and effective prevention strategy. The school takes a robust stance against sexual harassment and sexual violence.

2) ROLES AND RESPONSIBILITIES

The Designated Safeguarding Lead (DSL) will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies. The DSL in discussion with the Deputy Head Pastoral will:

- Ensure that all incidents of cyberbullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's Anti-bullying Policy, Behaviour Policy and Safeguarding and Child Protection Policy.

- Ensure that all policies relating to safeguarding, including cyberbullying are reviewed and updated regularly
- Ensure that all staff know that they need to report any issues concerning cyberbullying to the Designated Safeguarding Lead.
- Ensure that all staff are aware of the Prevent Duties.
- Provide training (using National College) so that staff feel confident to identify children at risk of being drawn into terrorism, to challenge extremist ideas and to know how to make a referral when a child is at risk.
- Ensure that parents/carers are informed and attention is drawn annually to the cyberbullying policy so that they are fully aware of the school's responsibility relating to safeguarding pupils and their welfare.
- Ensure that at the beginning of each term, cyberbullying is revisited as part of the tutor, PSHE and pastoral programme and that pupils know how to report a concern to someone on their circle of care, Childline or the thinkuknow website: **www.thinkuknow.co.uk**
- Ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond. All staff should sign to say they have read and understood the Acceptable Use Policy and Staff Code of Conduct.
- Give regard to the updates to KCSIE 2025 which highlights the 'four cs' of online risk from misinformation, disinformation and conspiracy theories.

The Online Safety Team (DSL and IT Manager) will:

- Ensure that all pupils are given clear guidance on the use of technology safely and positively both in school and beyond including how to manage their personal data and how to report abuse and bullying online.
- Ensure that all pupils' personal devices have certificates that allow the filtering and monitoring systems to work on them
- Provide annual training for parents/carers on online safety and the positive use of technology
- Ensure the school's Acceptable Use Policy, Online-Safety rules and ICT code of Conduct are reviewed annually
- Provide annual training for staff on the above policies and procedures
- Provide annual training for staff on online safety
- Plan and deliver a curriculum on online safety in computing lessons which builds resilience in pupils to protect themselves and others online.

- Plan a curriculum and support PSHE staff in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.
- Consider how generative AI and other new technologies are used by pupils and staff, including their filtering and monitoring responsibilities.
- Ensure adequate safeguards are in place to filter and monitor inappropriate content which will alert the online safety team to any misuse or inappropriate access. The school uses a third-party web-proxy solution to filter all internet access. The internet filter records access to prohibited sites which enables the Online Safety Team to act upon where appropriate.

The IT Manager will:

- Ensure the school manages personal data in line with statutory requirements. The school is aware of its duties under the Data Protection Act and General Data Protection Regulations (2018). Careful consideration will be given when processing personal information so that the individual's privacy is respected where it needs protection. Access to the personal information will only be given to those who need it. The principles of the Data Protection Act will be applied when processing, collecting, disclosing, retaining or disposing of information relating to a pupil or member of staff.

The Head of School and Director will:

- Ensure the policies and practices relating to safeguarding including the prevention of cyberbullying are being implemented effectively.

3) GUIDANCE FOR STAFF

Guidance on safe practice in the use of electronic communications and storage of images is contained in the Code of Conduct and Acceptable Use Policy (AUP). The school will deal with inappropriate use of technology in line with the Code of Conduct and AUP which could result in disciplinary procedures.

Useful websites for guidance can be found here:

- **Preventing Homophobic Bullying Among Children**
- **Department for Education Preventing Bullying Advice**
- **Ofsted Strategies for Tackling Bullying**
- **Embedding Anti-bullying Work in Schools**
- **Cyberbullying: Advice for Headteachers and School Staff**
- **Childnet's guidance**

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the pupil to save the message/image
- Inform the Deputy Head and Designated Safeguarding Lead immediately and pass them the information that you have

Computers

- Ask the pupil to get up on-screen the material in question
- Ask the pupil to save the material
- Print off the offending material straight away
- Make sure you have got all pages in the right order and that there are no omissions
- Inform the DSL and pass them the information that you have to them
- If DSL not available then use the reporting suspicious activity on the staff useful links page

Use of Technology in School

All members of the school community are expected to take responsibility for using technology positively. As well as training, the following is in place:

- All staff are expected to confirm they have read and understood the Acceptable Use Policy.
- All staff are expected to confirm they have read and understood the Staff Code of Conduct
- All children are expected to have been taken through and understood Online-Safety rules and ICT code of conduct.

When responding to cyberbullying concerns, the school will:

- Act as soon as an incident has been reported or identified.
- Provide appropriate support for the person who has been cyberbullied and work with the person who has carried out the bullying to ensure that it does not happen again.
- Encourage the person being bullied to keep any evidence (screenshots) of the bullying activity to assist any investigation.
- Take all available steps where possible to identify the person responsible. This may include:
    - Looking at use of the school systems;
    - Identifying and interviewing possible witnesses;
    - Contacting the service provider and the police, if necessary.
- Work with the individuals and online service providers to prevent the incident from spreading and assist in removing offensive or upsetting material from circulation. This may include:
    - Support reports to a service provider to remove content if those involved are unable to be identified or if those involved refuse to or are unable to delete content.
    - Confiscating and searching pupils' electronic devices, such as mobile phones, in accordance with the law and the school searching and confiscation policy. (The School will ensure they access the DfE **'Searching, screening and confiscation at school'** and **Childnet cyberbullying guidance** to ensure that the schools powers are used proportionately and lawfully)
    - Requesting the deletion of locally held content and content posted online if they contravene school behavioural policies.

- Ensure that sanctions are applied to the person responsible for the cyberbullying; the school will take steps to change the attitude and behaviour of the bully, as well as ensuring access to any additional help that they may need.
- Inform the police if a criminal offence has been committed. If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact: the local police or CEOP **(http://www.ceop.gov.uk/)**
- Provide information to staff and pupils regarding steps they can take to protect themselves online. This may include:
    - Advising those targeted not to retaliate or reply;
    - Providing advice on blocking or removing people from contact lists;
    - Helping those involved to think carefully about what private information they may have in the public domain.

4) GUIDANCE FOR PUPILS

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff on your circle of care.

- Do not answer abusive messages but save them and report them
- Do not delete anything until it has been shown to your parents/carers or a member of staff at school (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal details or contact information without the permission of a parent/guardian (personal data)
- Be careful who you allow to become a friend online and think about what information you want them to see
- Protect your password. Do not share it with anyone else and change it regularly
- Always log off from the computer when you have finished or if you leave the computer for any reason.
- Always put the privacy filters on to the sites you use. If you are not sure how to do this, ask a teacher or your parents.
- Never reply to abusive e-mails
- Never reply to someone you do not know
- Always stay in public areas in chat rooms
- The school will deal with cyberbullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.

- Report any concerns of cyber bullying to either the DSL or using the anonymous reporting button on the pupil's useful links page.
- The school will deal with inappropriate use of technology in the same way as other types of inappropriate behavior and sanctions will be given in line with the school's Behaviour Policy
- There is plenty of online advice on how to react to cyberbullying. For example, useful tips can be found at: **https://www.familylives.org.uk/advice/bullying/cyberbullying** and **www.wiredsafety.org**

Specific advice:

Text/video messaging

- You can easily stop receiving messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you as you won't respond to them
- If the bullying persists, you can change your phone number or messaging accounts. Ask your mobile service provider or a teacher/parent to help with this
- Don't reply to abusive or worrying text or video messages. Your mobile service provider or Social Media website will have a number for you to ring or text to report phone bullying
- Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence
- Text harassment is a crime. If the calls are simply annoying, tell a teacher or parent. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received

Phone calls

- If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise, they can't get you rattled, callers usually get bored and stop bothering you
- Always tell someone else: a teacher or parent
- Be careful to whom you give personal information such as your phone number especially online forms – a free prize giveaway is rarely free as they want your personal information in return
- If you have a mobile phone, make sure you set a passcode then others cannot use your phone to send a message once the phone is locked

- Never reply to unpleasant or unwanted emails ('flames'): the sender wants a response, so don't give them that satisfaction
- Keep the emails as evidence. Tell an adult about them
- Ask an adult to contact the sender's Internet Service Provider (ISP)
- Never reply to someone you don't know, even if there's an option to 'unsubscribe'. Replying simply confirms your email address as a real one

Web Bullying

- If the bullying is on a website (e.g. Facebook), tell a teacher or parent, just as you would if the bullying were face-to-face – even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this
- Chat rooms and instant messaging
- Never give out your name, address, phone number, school name or password online
- It's a good idea to use a nickname. Don't give out photos of yourself
- Don't accept emails or open files from people you don't know. Remember it might not just be people your own age in a chat room
- Stick to public areas in chat rooms and get out if you feel uncomfortable
- Tell your parents or a teacher if you feel uncomfortable or worried about anything that happens in a chat room
- Think carefully about what you write or say; don't leave yourself open to bullying
- Don't ever give out passwords to your mobile or email account

Three steps to stay out of harm's way:

- Respect other people, both online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords
- If someone insults you online or by phone, stay calm, and ignore them
- 'Do as you would be done by.' Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else

5) GUIDANCE FOR PARENTS/CARERS

It is vital that parents/carers and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. Parents/carers must play their role and take responsibility for monitoring their child's online life.

- Parents/carers can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
- Parents/carers should also explain to their children legal issues relating to cyber-bullying.
- If parents/carers believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving the offensive text on their computer or on their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents/carers should contact the school as soon as possible.
- If the incident falls in the holidays the school reserves the right to act against bullying perpetrated outside the school both in and out of term time.

The school will ensure parents/carers are informed of the cyber-bullying policy for children and the procedures in place in the Anti-Bullying Policy to deal with all forms of bullying including cyber-bullying.

There is a dedicated and regularly updated internal website, accessible on the parent portal to provide guidance on online-safety for parents, staff and pupils:

https://sites.google.com/boundaryoakschool.co.uk/esafety/home

E-Safety at Home

Several sites offer helpful advice to parents/carers, particularly with respect to how they can best monitor their child's use of the computer at home. Here are some parents/carers might like to try:

- **www.thinkyou.know.co.uk/parents**
- **www.saferinternet.org.uk**
- **Vodafonedigitalparenting.co.uk**
- **www.childnet.com**
- **www.anti-bullyingalliance.org.uk**

- **www.nspcc.org.uk**
- **www.cyberangels.org**
- **Digizen**
- **DfE Advice for Parents on Cyberbullying**
- **Childnet Cyberbullying Leaflet**
- **DfE The use of social media for on-line radicalisation**
- **http://www.bullying.co.uk/cyberbullying/**
- **www.wiredsafety.org**
- **Family Online Safety Guide.**
- **Childnet International SMART rules**
- **Internet Watch Foundation**
- **Children's Commissioner guidance on how parents should talk to their children about online sexual harrassment**

This is a Whole School policy and relates to EYFS and Boarding.

For further references, please refer to the Boundary Oak School Anti-Bullying Policy.