



HOLMEWOOD HOUSE SCHOOL

CYBERBULLYING POLICY

Policy Holder	Assistant Head, Pastoral and Wellbeing
Date Approved	September 2026
Governor Approval	E&P Committee
Date for next review	September 2027

This policy should be read in conjunction with:

- Acceptable Use of Technology
- BYOD – pupils use of devices in school
- Online Safety Policy
- The use of smart technology including mobile phones
- Safeguarding Policy

This is a whole school policy and applies to EYFS

This policy should be read in conjunction with our:

- Anti-bullying Policy
- Behaviour Policy
- Safeguarding and Child Protection Policy (including Prevent)
- Staff Code of Conduct

Holmeewood House 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.

CYBERBULLYING

Cyberbullying may be defined as ‘the use of electronic communication, particularly mobile phones and the internet, to bully a person, typically by sending messages of an intimidating or threatening nature: children and adults may be reluctant to admit to being the victims of cyberbullying’. It can take a number of different forms: threats and intimidation, harassment or ‘cyber-stalking’ (e.g. repeatedly sending unwanted texts or instant messages), sexting (e.g. sending and receiving sexually explicit messages, primarily between mobile phones) vilification/defamation, exclusion/peer rejection, impersonation, unauthorised publication of private information/images and ‘trolling’ (abusing the internet to provoke or offend others online). It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

However, it differs from other forms of bullying in several significant ways:

- by facilitating a far more extreme invasion of personal space. Cyberbullying can take place at any time and intrude into spaces that have previously been regarded as safe and personal
- the potential for anonymity on the part of the bully. This can be extremely distressing for the victim
- the potential for the bully to play very rapidly to a larger audience so the scale and scope of cyberbullying can be greater than for other forms of bullying
- through the knowledge that the data is in the world-wide domain, disproportionately amplifying the negative effect on the victim, even though the bully may feel his / her actual actions had been no worse than conventional forms of bullying
- the difficulty in controlling electronically circulated messages as more people get drawn in as accessories. By passing on a humiliating picture or message a bystander becomes an accessory to the bullying
- the profile of the bully and target can be different to other forms of bullying as cyberbullying can take place between peers and across generations. Teachers can be victims and age and size are not important
- many cyberbullying incidents can themselves act as evidence, so it is important the victim saves the information

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).

Keeping Children Safe in Education 2026

- Under KCSIE 2026, schools have a responsibility to take cyberbullying seriously as part of their wider safeguarding, behaviour and online-safety duties. It states schools should have clear measures in place for preventing and responding to bullying, including bullying that takes via social media, messaging platforms, gaming or other online or mobile phone spaces.
- Schools should also provide age-appropriate education that helps pupils understand respectful relationships, online behaviour, harmful content, harassment and how to seek help. Effective filtering and monitoring arrangements are an important part of creating a safe digital environment, but no technical system is 100% effective, so staff remain an essential part of identifying and responding to concerns.

Preventing and Responding to Cyberbullying

This is a whole school policy which also applies to Early Years Foundation Stage and Boarding

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:

ROLES AND RESPONSIBILITIES

The Assistant Head (Pastoral Care & Wellbeing and DSL)

Will take overall responsibility for the coordination and implementation of cyberbullying prevention and response strategies. The Assistant Head (Pastoral Care & Wellbeing) 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.
- provide annual training or information for parents/carers on online safety and the positive use of technology.
- ensure the school's Acceptable Use Policy and e-Safety Policy reviewed annually.
- provide annual training for staff on the above policies and procedures.
- provide annual training for staff on online safety.
- 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 EduCare and/or KCC Education People provided training) 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. The Designated Safeguarding Lead is also the Designated Prevent Lead.
- 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. The Cyberbullying Policy is always available on the school website
- ensure that all parents/carers and pupils receive a copy of the Cyberbullying Leaflet. This is always available on the school website. Parents/carers should take younger children through the leaflet.
- ensure that each year, cyberbullying is revisited as part of the MHMMMW / IT curriculums and that pupils know how to report a concern. (to someone on their safety circle, Childline or the 'thinkuknow' website: www.thinkuknow.co.uk)
- ensure that all staff are aware of their responsibilities by providing clear guidance for them on the use of technology within school and beyond. All staff should sign to say they have read and understood the Staff Code of Conduct.

The Strategic Technology Manager

Will:

- ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Lead to safeguarding issues. 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 Designated Safeguarding Lead to monitor what the pupils and staff are accessing online.
- To complete a full test of the Smoothwall filtering and monitoring software each year in order to ensure it is as effective as possible and new trends or use of IT is included, including use and access to AI programmes.
- Ensure that visitors to the school are given clear guidance on the use of technology in school. This includes how to report any safeguarding issues to the Designated Safeguarding Lead. Visitors will be given highly restricted guest accounts which will not allow any access to personal data and that any misuse of the system will result in access to the system being withdrawn.

The Bursar

- Will ensure the school manages personal data in line with statutory requirements. The school is aware of its duties under the Data Protection Act (1998). 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 School Governors

- Will Appoint a governor in charge of Safeguarding who will work with the Designated Safeguarding Lead to ensure the policies and practices relating to safeguarding including the prevention of cyberbullying are being implemented effectively. The current Safeguarding Governor is Alex Patton.

GUIDANCE FOR STAFF

Guidance on safe practice in the use of electronic communications and storage of images is contained in the Code of Conduct. The school will deal with inappropriate use of technology in line with the Code of Conduct which could result in disciplinary procedures. Staff receive regular reminders and updates on the process of reporting any suspected incident and use the protocol outlined below:

Mobile Phones

- Carry out an initial review meeting:
- 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 (or one of the DSL team in their absence) immediately and pass them the information that you have.

Computers

- Ask the pupil to get up on-screen the material in question (if a nude or semi-nude image, please see below)
- Ask the pupil to save the material, e.g. take a screenshot.

- 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 a member of the Senior Leadership Team and pass them the information that you have.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Nude and Semi-Nude Images

Following a disclosure of a nude or semi-nude image, the following guidelines should be followed

Sharing nude and semi- nude images advice

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 sign to confirm they have read and understood the Acceptable Use Policy.
- All staff are expected to sign to confirm they have read and understood the Staff Code of Conduct.
- All children are expected to have been taken through and understood Acceptable use of Technology Policy

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 safety network.

- 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.

- The school will deal with inappropriate use of technology in the same way as other types of inappropriate behaviour and sanctions will be given in line with the school's Behaviour Policy.

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. Please contact:
 - sporter@holmewoodhouse.co.uk – Simon Porter, Assistant Head (Pastoral Care & Wellbeing) & DSL
 - Cwukics@holmewoodhouse.co.uk – Caolan Wukics, Boarding DSL
 - afaure@holmewoodhouse.co.uk – Antoinette Faure, Pre Prep & EYFS DSL
 - Vbarwick@holmewoodhouse.co.uk – Victoria Barwick, Medical Centre, DSL
- If the incident falls in the holidays the school reserves the right to take action against bullying perpetrated outside the school both in and out of term time.
- DSL coverage is in place all year round, with the lead DSL being the first point of call and other listed DSL's having their contact details listed if needed.
- Parents/carers should attend the school's annual training on online safety organised by the Deputy Head Pastoral and the Designated Safeguarding Lead or read the information sent out.

Parents are responsible for ensuring their child/ren's devices do not return to school containing any inappropriate material. This applies to both day pupils and boarders. Their devices should not be able to bypass the school's filtering system through the use of VPNs or mobile data. Spot checks will be carried out on pupils' devices and appropriate education or sanctions put in place where needed. Parents will be informed.

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

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
- Vodafone.digitalparenting.co.uk
- www.childnet.com
- www.anti-bullyingalliance.org.uk

- www.nspcc.org.uk
- www.cyberangels.org
- [Digizen](#)

The following useful publications may be of further interest:

- [DfE The use of social media for on-line radicalisation](#)

Other publications:

- [Sharing nude and semi-nude images](#)

ADDITIONAL SAFEGUARDING CONTACT INFORMATION

The Designated Safeguarding Lead, Assistant Head – Simon Porter sporter@holemwoodhouse.co.uk
 Safeguarding Governor, Welfare and Prevent Duty – Alex Patton atp@kings-school.co.uk
 Safeguarding Governor, Digital and Online Safety – Olivia Upchurch oupchurch@brightoncollege.net