REVIEWED: AUTUMN 2023
NEXT REVIEW DATE: AUTUMN 2024
REVIEWED BY: DEPUTY HEAD
RATIFIED BY: EDUCATION COMMITTEE

Hazelwood School

Cyberbullying Policy

This Policy includes the Early Years Foundation Stage

Aims and Objectives:
Hazelwood School has a duty to protect pupils and staff from mobile and smart technology that is harmful and damaging and which can, in some circumstances, constitute a criminal act.

Cyberbullying may be defined as the use of electronic communication, particularly mobile phones and the internet to bully a person, by sending messages of an intimidating or threatening nature. Bullying is never acceptable, and Hazelwood fully recognises its duty to protect all of its members and to provide a safe, healthy environment for everyone. Hazelwood has a clear framework of policies giving guidance in this area and also ensures that pupils and staff are inducted into the School's Expectations on arrival. In addition, we are committed to providing an effective, age-appropriate, and on-going programme of education throughout the time the children are at the School.

Cyberbullying is a form of child-on-child abuse. It is important that all staff recognise the indicators and signs of child-on-child abuse and know how to identify it and respond to reports, as outlined in the Safeguarding Policy.

There is a clear system of sanctions in place for those who fall short of our expectations. This Policy outlines in greater detail how pupils, parents and staff can work together to foster an environment in which cyberbullying is not tolerated and where there is effective detection of and sanction for those involved in cyberbullying.

Online Safety
When children use the School's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. However, many pupils can access the internet using their own data plan. To minimise inappropriate use, as a school we ensure that children are taught about safeguarding, including online safety as part of our broad and balanced curriculum. Additionally, Hazelwood provides information and presentations for parents to help support families staying safe online.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

● content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

● contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

● conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

● commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Reference to Other School Policies and Guidance:
This Cyberbullying Policy should be read in conjunction with the below:

- Safeguarding and Child Protection Policy
- Acceptable Use Policy (either Pupil, Staff or Guest as appropriate)
- Anti-Bullying Policy
- E-Safety Policy
- Personal, Social, Health and Economic Education (PSHE) programme
- Staff Code of Conduct
- Staff Code of Conduct Addendum

Guidance for Pupils

1. Always respect others – think about what you say online and what images you send/post.
2. Remember that anything you publish online can be made public very quickly and you will never be sure who may have seen it. Once something is posted you lose control.
3. Treat your password carefully – never share it with anyone and only give your personal information like mobile phone number or email address to trusted friends.
4. Learn how to block or report online bullies or anyone behaving badly.
5. Do not retaliate or reply to nasty messages, instead talk to a trusted adult.
6. Save any evidence if possible e.g. – text messages, online conversation, pictures etc.
7. If you witness cyberbullying, always report it to a member of staff or trusted adult.
8. Avoid using anonymous websites (such as ask.fm).

Guidance for Parents

- Role model positive online behaviour for your child. It is important that they know how to act safely and responsibly online and are aware of what content is acceptable and unacceptable to post or share.
- Talk to your child and understand how they are using the internet, phone, tablet or other device.
- Use safety tools and parental controls – if you are not sure how, contact your service provider but please note that these tools are not always 100% effective.
- Remind your child not to retaliate to any cyberbullying, notify the Senior Leadership Team, we always take bullying in any form seriously.
- Work with the School to resolve the issue if other pupils are involved.
- Keep any evidence of cyberbullying – emails, online conversations, texts, screenshots of sites/chat messages – try and include time/date etc.
- Report the cyberbullying:
    - Contact the service provider (e.g. the website, gaming site or mobile phone company) to report the user and if possible to remove the content.
    - Contact the School so they can take action if it involves another pupil.
    - If the cyberbullying is serious and a potential criminal offence has been committed, then consider contacting the police.
- Further advice regarding cyberbullying can be found at:

  https://www.thinkuknow.co.uk/parents/;www.saferinternet.org.uk;
  https://www.nspcc.org.uk/ DfE publication Advice for parents and carers on cyberbullying (Nov 2014).

Guidance for Staff

- Keep all passwords and login details secret.
- Make sure you understand how to secure any websites or social networking services you use and have read the School Social Networking (Staff) Policy.
- Always think carefully before you post and do not post any information (photos, videos, comments) publicly online that you would not want employers, colleagues, pupils or parents to see. Just because a profile might be set to "private" it does not mean that

someone else cannot copy or share it without your knowledge.

- Also consider if it could bring you, the School or someone else's reputation into disrepute. Posting something unsafe, inappropriate, obscene or threatening online could lead to criminal, civil and/or disciplinary action.
- Staff are not to add or friend pupils (past or present) or their parents on any personal social networking accounts. Discuss any issues with this (for example any pre-existing relationships) with the School.
- Do not use your own personal devices or personal social networking profiles to contact pupils or parents.
- Ensure that the School's rules and policies regarding the use of technologies by pupils and staff are enforced. Make sure you read and understand the School's eSafety Policy and procedures.
- Do not personally retaliate to any incidents which involve yourself or other members of staff.
- Always report any incidents of cyberbullying witnessed (either of yourself or other staff members) in a timely manner.
- Make sure you save and keep any evidence of cyberbullying e.g. screenshots. Screenshots are not to be taken of sexually explicit material.
- Further advice is available in the DfE document – Cyberbullying: Advice for head teachers and school staff (Nov 2014).

To be used in conjunction with iPad AUP Policy, Acceptable Use of ICT, Mobile Phones and other Electronic Devices Policy, and Safeguarding Policy

Ratified by the Education Committee on the 15 November, and noted by the Compliance Committee on the 24 November 2023