FIDES et OPERA

BROMLEY

HIGH SCHOOL

GDST

GIRLS' DAY SCHOOL TRUST

Anti-Bullying Policy- Cyberbullying Annex

The school's response to cyberbullying, both preventive and reactive, is integrated into its response to its anti-bullying work as a whole, as outlined in the main Anti-Bullying Policy. However, there are some points that are specific to online abuse which are covered in this annex.

What do we mean by cyberbullying?

Cyberbullying can be defined as:

'the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else'[1]

The use of technology as a tool for bullying has increased significantly and, inevitably, changes rapidly as technology use and trends evolve. This kind of bullying can be particularly devastating to the person being bullied, as they are unable to escape the (sometimes anonymous) perpetrator(s) as the taunts and intimidation follow them home, invade their personal space, and can extend to a wide audience. Single incidents of abuse can quickly escalate into cyberbullying by reposting, sharing and commenting, and once something is posted on the internet it is likely to leave a lasting digital trail.

Cyberbullying is not a rare occurrence. A report from Public Health England showed that 17.9% of 11-15 year olds had experienced cyberbullying in the two months prior to being surveyed[2]. It also found that cyberbullying increased with age, but that it does not create a large number of new targets – it tends to be a modern tool used to supplement traditional forms of bullying.

The school regards this type of bullying very seriously and will take action whether reported cyberbullying takes place in or out of school, during or outside school hours. The Education Act 2006 includes legal powers that allow the Head to regulate the behaviour of pupils when they are off site. Any disrespectful or inconsiderate behaviour online is both wrong and in direct contravention of the school's Acceptable Use Agreements. Furthermore, criminal laws apply to a range of behaviours linked to cyberbullying including stalking, threats, accessing computer systems without permission, and circulating sexual images. Where cyberbullying could potentially constitute a crime, the school will report the case to the police.

AI and Deepfake Abuse

[1] Cyberbullying: Understand, Prevent and Respond – Guidance for schools (Childnet International)

[2] Cyberbullying: An analysis of data from the Health Behaviour in School-aged Children (HBSC) survey for England, 2014

The school recognises the growing risks posed by artificial intelligence, particularly the creation and misuse of deepfake content. Deepfakes, or digitally altered images, videos or audio designed to mislead or impersonate could be used to bully, harass, or damage reputations. Such behaviour is strictly prohibited and will be treated as a serious safeguarding or behavioural concern. Pupils are educated about the ethical use of AI and encouraged to report any incidents involving AI-generated abuse.

Forms of cyberbullying

There are many forms that cyberbullying can take, including:

- Threats and intimidation by mobile phone, email, within online games, or via comments on websites, social networking sites or message boards
- Harassment or stalking, e.g., by repeatedly sending unwanted messages or making calls (including silent calls) – or using public forums to post derogatory or defamatory statements.
- Vilification/defamation – including posting upsetting or defamatory remarks about an individual, or name-calling and general insults
- Ostracising/peer rejection/exclusion – e.g., setting up a closed group to deliberately exclude an individual, excluding people from online conversations, or talking behind their back
- Identity theft / unauthorised access and impersonation
- Publicly posting, sending or forwarding personal or private information or images
- Artificial Intelligence-driven online abuse such as deepfake images and videos, voice-cloned calls, algorithmically generated hate speech, and bot-driven harassment campaigns

Cyberbullying is often linked to discrimination, including on the basis of sex, race, faith, sexual orientation, gender identity or special educational needs and disabilities. Girls report experiencing a higher incidence of cyberbullying than boys, and in particular are disproportionately subject to online sexual harassment.

Protecting yourself from cyberbullying

Following good online safety precautions can, to some extent, protect you from online bullying. Privacy settings should be kept up to date and personal information such as mobile numbers and email addresses only shared with trusted friends. It is also advisable to monitor your screen time and avoid dependence on social media – which is designed to be addictive.

You should also consciously protect yourself from being drawn into bullying others online. It is far easier to post or send an unkind electronic message than to say something hurtful face to face. Initial incidents can have unintended consequences, and one upsetting post or message may escalate into cyberbullying involving many people over time. Cyberbullying also attracts virtual bystanders, i.e., those who participate in the abuse through their involvement in online surveys and discussion groups, or by passing on images or messages. This adds to the humiliation felt by the person being bullied and will be treated as collusion in bullying by the school.

The school's response to cyberbullying, both preventive and reactive, is integrated into its response to its anti-bullying work as a whole, as outlined in the main Anti-Bullying Policy. However, there are some points that are specific to online abuse which are covered in this annex.

What to do if you are being bullied online

Whatever form bullying takes, it is very important to report it to a member of staff, parent or other adult you trust. There are also anonymous reporting routes you can use such as the "Confide" button on your home screen or, in the junior school, Listening Ear Box.

Do not retaliate or return the message. However, you should keep a record of abusive incidents, particularly: the date and time, content of the message(s), and where possible the sender's ID or the web address of the content and a screenshot. Keeping evidence will be important in identifying the perpetrator(s) and taking action to stop the bullying. You can also block abusive contacts and consider changing your user ID, nickname or profile.

Do not retaliate or return the message. However, you should keep a record of abusive incidents, particularly: the date and time, content of the message(s), and where possible the sender's ID or the web address of the content and a screenshot. Keeping evidence will be important in identifying the perpetrator(s) and taking action to stop the bullying. You can also block abusive contacts and consider changing your user ID, nickname or profile.

What the school will do

If a cyberbullying incident does not constitute a criminal offence, the school will take steps to contain it by removing upsetting material from devices and services as quickly as possible. If the incident does constitute a criminal offence, it will be reported according to the relevant protocols and the evidence secured appropriately.

The school can confiscate, retain or dispose of a pupil's devices as a disciplinary penalty, where this is reasonable. The Head and members of staff formally authorised by the Head can search a pupil's device without consent if there are reasonable grounds that it contains items specified as prohibited [note these powers only apply in England]. Locally held content can be deleted, if it is not to be retained as evidence.

Cyberbullying of staff

The school has a responsibility to safeguard staff as well as pupils against the threat of cyberbullying. Malicious conduct against staff online will be pursued with the same vigour as that against pupils. Staff are reminded of the importance of keeping privacy and security settings up to date, regularly checking their online presence, and observing the guidelines in the Social Media Policy. Any member of staff subject to online abuse should keep evidence of the incident and report it to their line manager or a senior member of staff as soon as possible.

Advice for parents

Protect your daughter by making sure she understands how to use technology safely and knows about the risks and consequences of misuse and be open and curious about your

child's activity online, so that she feels she can talk to you if something goes wrong. There are also safety features you can install on devices to help protect the user.

If you are concerned, search your daughter's name online, look at her profiles and posting on social media and community sites, review web pages or blogs, and watch out for nervous or secretive behaviour, such as rapidly switching screens or displaying anxiety when being kept away from the internet, and for attempts to hide online behaviour, such as empty file history. Be aware that your child may as likely cyberbully as be a target of cyberbullying. If you suspect or discover that your child is cyberbullying or being cyberbullied, contact the school. Parents can also take action by reporting abusive content to service providers or social networking sites.

Further sources of advice and support

Cyberbullying: understand, prevent and respond (Childnet)

Cyberbullying: advice for headteachers and school staff (DfE)

Advice for parents and carers on cyberbullying (DfE)

Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)

Anti Bullying Alliance – collates resources from member organisations in one place and includes pages for schools, parents and young people. Cyberbullying section: https://www.anti-bullyingalliance.org.uk/tools-information/all-about-bullying/online-bullying

CEOP for making a report about online abuse

UK Safer Internet Centre for reporting and removing harmful online content

Report Remove – Childline's service to help those under 18 get a nude image of themselves removed

Take it down – a tool from the National Centre for Missing and Exploited Children for removing or stopping the online sharing of images or videos

Professional Online Safety Helpline (POSH) Tel: 0344 381 4772

Education Support Partnership Tel: 08000 562 561

Stop Online Abuse provides advice for women and LGBTQIA+ people