Cyberbullying Policy

Date Reviewed: November 2017

Date Ratified by Governors: December 2017

Date due for renewal: November 2018

Introduction
This Policy should be used in conjunction with the e-safety and Anti Harassment and Bullying Policies.

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 an 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 recognizes its duty to protect all of 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:

Roles and Responsibilities
The Assistant Head who is also the Designated Safeguarding Assistant Lead will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies. The Assistant Head 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. E-safety Policy and Safeguarding 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 Leads.
- 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 available at all times on the school website.

The Network Manager will:
- Ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Leads to safeguarding issues. The school uses Impero to filter all internet access. Impero records access to prohibited sites, which enables the IT Support Team to report issues immediately to the Designated Safeguarding Leads.

Guidance for Staff

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 Assistant Head and Assistant Head 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 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.

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.
- 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.
- 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 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 cyberbullying.
- 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.

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:

- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf
- https://www.thinkuknow.co.uk/parents/
- www.saferinternet.org.uk
- www.anti-bullyingalliance.org.uk