LIME HOUSE SCHOOL

Cyberbullying Policy (09/05/2018)

This is a whole school policy and applies to EYFS and Boarding
This policy should be read in conjunction with the Anti-bullying Policy, the Behaviour Policy, the Child Protection (Safeguarding) Policy and Sexting Policy.

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.

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), 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 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. (See the Behaviour Policy)

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 Headteacher and Ultimate Designated Safeguarding Lead (Mrs Rice) will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies. The DSL 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 Channel online awareness training module) 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 Deputy Head 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 available at all times on the school website

• ensure that at the beginning of each term, cyberbullying is revisited as part of the Staying Safe Programme 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 staff 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. (Found in the Child Protection (Safeguarding) Policy.

The Head of Computing 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 the school's Internet Safety and Internet Use policies 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 PSE staff in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

The School's Network Service Providers will
• ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Head of Computing to safeguarding issues. The school uses OpenDNS to filter all internet access. Lightsquid records access to prohibited sites which enables the Network Service Provider to report safeguarding issues to the Head of Computing who informs the Designated Safeguarding Lead.
• 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 access to 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. They may also be given internet access for BYO devices which use the school firewall software.

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 Proprietors will
• conduct an annual review of the cyberbullying policy.

Guidance for Staff

All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times.

• Ensure you understand your school's policies on the use of social media, Childnet's 'Using Technology' guide has more information on what to be aware of.

• Do not leave a computer or any other device logged in when you are away from your desk.

• Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by pupils.

• Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the Safer internet advice and resources for parents and carers.

• It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centres Reputation minisite has more information on this.

• Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.

• Consider your own conduct online; certain behaviour could breach your employment code of conduct.

• Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.

• Do not accept friend requests from pupils past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.

• Do not give out personal contact details – if pupils need to contact you with regard to homework or exams, always use your school's contact details. On school trips, staff should have a school mobile phone rather than having to rely on their own.

• Use your school email address for school business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

If you are bullied online

• You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.

• Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.

• Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.

• Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.

• If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.

• If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.

• Employers have a duty to support staff and no-one should feel victimised in the workplace. Staff should seek support from the senior management team, and their union representative if they are a member.

• The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

• The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

Guidance for staff who witness cyberbullying.

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 a member of the Senior Management 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.

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 Staff Behaviour policy/code of conduct (found in the Child protection (Safeguarding) Policy.
• All staff are expected to have read and understood the Behaviour Policy Guidelines for the 'Confiscation of Inappropriate Items'.
• All children are expected to have been taken through and understood the Children's Internet Acceptable Use 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. For more advice, look at the Cyberbullying leaflet.

 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 Mrs Robertson-Barnett, Mrs Rice or Mrs Fisher on 01228 710225

 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.

 Parents/carers should attend the school's annual training on online safety delivered by the Head of Computing.

The school will ensure parents/carers are informed of the cyber-bullying policy and other relevant policies.

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
• www.childnet.com
• www.anti-bullyingalliance.org.uk
• www.nspcc.org.uk
• www.cyberangels.org
• Digizen

The following are useful online publications.
• DfE Advice for Parents on Cyberbullying
• Childnet Cyberbullying Leaflet
• DfE The use of social media for on-line radicalisation

This policy was reviewed and updated in August 2018 and will be reviewed in August 2019 or sooner if new legislation applies.

N A Rice MA
School Proprietor