HUNTER HALL SCHOOL

CYBER BULLYING (Safeguarding) POLICY

Compiled	Head teacher	February 2015	D Vinsome
Reviewed	Head teacher	March 2015	D Vinsome
Approved	SG Governor	April 2015	A Hill
Amended	Head teacher	May 2015	D Vinsome
Reviewed and amended	Head teacher / MS	November 2015	D Vinsome/M Spooner
Approved	SG Governor	November 2015	C Young
Amended	Head teacher	November 2016	D Vinsome
Approved	SG Governor	November 2016	C Young
Amended	Head teacher	Sept 2017	D Vinsome
Approved	SG Governor	Sept 2017	C Young
Amended	Head teacher	Sept 2018	D Vinsome
Approved	SG Governor	Sept 2018	C Young

Amended	Head teacher	Oct 2019	D Vinsome
Approved	SG Governor	Oct 2019	L Millburn
Amended	Head teacher	Sept 2020	D Vinsome
Approved	SG Governor	Oct 2020	L Millburn
Amended	Head teacher	Oct 2021	D Vinsome
Approved	SG Governor	Oct 2021	L Millburn
Amended	Head teacher	Oct 22/Jan 23	D Vinsome
Approved	SG Governor	Jan 23	G B

Cyber-bullying

This policy is written in conjunction with advice given in ISI regulatory requirements – Part 3 'Welfare, Health and Safety of Pupils' and KCSIE Sept 2022. It is also written with regard to 'The Use of Social Media for on-line radicalisation' (July 2015) 'The Prevent Duty' June 2015 Cyberbullying; advice for head teachers and school staff (2014)
It may be read in conjunction with our Safeguarding policies – particularly Anti-Bullying, Behaviour and sanctions, and child protection policies.
It may also be useful to refer to our ICT subject handbook.

At Hunter Hall we aim to instil in our children the good sense to know what is available to them electronically and the risks to which they may be subject.

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' cyber-bullying, which can **occur in or outside school**. Cyber-bullying is a form of bullying and can happen at all times of the day to all children(including those classed as more vulnerable and with 'protected characteristics' such as those with special educational needs, disabilities looked after and adopted children, different ethnic groupings, LGBT, and those with alternative family provision, with a potentially bigger audience, as people forward on content at a 'click'.

Cyberbullying includes:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations.
- exposing children to radicalisation and extremist activity

Cyberbullying and the law
While there is not a specific criminal offence called cyberbullying, activities can be criminal offences under a range of different laws, including:

- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988,
- Section 127 of the Communications Act 2003
- Public Order Act 1986
- The Defamation Acts of 1952 and 1996
- The prevent Duty 2015
- The equality Act 2010

The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones. (see electronic device user agreement)

All members of Hunter Hall, both staff and children from our EYFS through to Year 6, have rights and responsibilities in relation to cyberbullying. Our aim is to work together to create an environment in which pupils can learn how to stay safe online as well as offline, and staff can have fulfilling careers free from harassment and bullying.

It is **completely unacceptable** for pupils, parents or staff to denigrate and bully via social media, text messages, email, etc. in the same way that it is unacceptable to do so face to face, peer on peer (see anti-bullying policy). At Hunter Hall we expect all members of the school community to use social media and messaging responsibly. Children are taught to do so through structured ICT lessons as well as covering modules relating to keeping yourself safe online in PSHE and through assemblies. Staff are kept informed of their duties at INSET/staff meetings and through signing their electronic usage agreement each academic year.

Our children are not allowed mobile phones onsite in school.

Please note that Hunter Hall School has robust filters in place in order to minimise the risk of terrorist and extremist material appearing on line when children have access to the internet and works closely with our internet providers to make us cybersecure.

In addition school usage is ***actively monitored*** by our DSL's using SENSO in response to recommendations in KCSIE.

Active management of hardware, software and connectivity and the vigilance of teachers and parents have a part to play in the safeguarding and protection of pupils and themselves.

What staff need to be aware of and do to help prevent cyberbullying as an educational professional.

1. ***Understand the software/sites*** *etc:* be aware of the reporting mechanisms (see below) on different sites and services so you can support children/parents/adults in making a report.
2. ***Discuss cyberbullying****:* be proactive in discussing cyberbullying with your pupils; how it occurs, why it occurs, and the consequences of such behaviour.
3. ***Know who to report to****:* Depending on the severity, either report cyberbullying to the child's form teacher or to the ***DSL immediately where you feel there may be a child protection issue and the child is likely to suffer significant harm from such bullying***. Appropriate action can then be decided. If a child discloses it is happening at home it may be prudent to talk to parents following advice from the DSL.
4. ***Know that cyberbullying may be more prevalent against those who have protected characteristics;*** for example race, religion, culture, sex, gender, homophobia, SEND and disability, or those children who have alternative home backgrounds for eg. been adopted or have a carer

What advice should staff give to HH pupils?

The internet is an amazing resource and can be used in a number of positive ways. However, content posted online can be easily misunderstood by others and taken out of context. It is important for children to recognise the importance *of* ***'thinking before you post'*** and the need to respect their friends' and peers' thoughts and feelings about things posted online. What's considered morally right and wrong offline must also be thought of in the same way online, and treating others with respect on the internet is a good way to ensure that online situations are less likely to escalate into cyberbullying situations.

Good advice for pupils includes:

1. ***Don't reply****:* most of the time the bully is looking for a reaction when they're teasing or calling someone nasty names. Remind children not to reply, if they do they're giving the bully exactly what they want.
2. ***Save the evidence****:* encourage children to save the evidence of any emails or text messages they receive. This is so they have something to show when they do report the cyberbullying.
3. ***Tell someone****:* encourage the children to tell a trusted adult if they are being cyberbullied or know of someone who is and they are a bystander and to tell them to do it as soon as they can in order to minimise their own upset or worry.

The aim is that by informing children of how they can help protect themselves we are helping children to become resilient, independent children.

School staff responsibilities:

All staff at school are in a position of trust, and there are expectations that they will act in a professional manner at all times. Key requirements for staff which help protect their online reputation include:

- Ensuring they have read and understand the school's safeguarding policies, including staff code of practice.
- Not leaving a computer or any other device logged-on when away from their desk.
- Ensuring they have enabled a PIN or passcode to protect themselves from losing personal data and images (or having them copied and shared) from their mobile phone or device if it is lost, stolen, or accessed by pupils.

What can staff expect if they are the victims of cyberbullying?

Hunter Hall takes seriously its duty to support school staff in order to ensure that no-one should feel victimised in the workplace. Staff should seek support from the senior management team if they ever feel they are the victim of on-line bullying. Staff should expect the school to react quickly to reported incidents and support the member of staff concerned to do so. A member of staff who is harassed in this way will receive support and information enabling them to access appropriate personal support. Where appropriate, the school will endeavour to approach internet providers or other agencies on their behalf, in order to request that the inappropriate material is removed. However, the internet provider may only accept a request from the victim and therefore the person being bullied will need to contact the service providers directly, with support from the school. This might apply, for example, in cases of identity theft, impersonation or abuse via a mobile phone service.

Staff must take steps to protect themselves and their personal information by:

- Keeping passwords secret and protecting access to their accounts.
- Never 'friending' pupils on personal social networking services.
- Keeping personal phone numbers private and wherever possible (unless given permission by the Head teacher) not using their own mobile phones to contact parents.
- ***Never*** ringing pupils directly – always speak to parents.
- Keeping a record of their phone's unique International Mobile Equipment Identity (IMEI) number, and keeping phones secure while on school premises. Personal mobile phones should never be visibly accessible to children or staff in the classroom. (see electronic user agreement and staff code of practice).
- Thinking before posting information about themselves publicly that they wouldn't want employers, colleagues, pupils or parents to see and that may bring the school into disrepute.
- Ensuring that rules regarding the use of technologies in school are consistently enforced.

- Not retaliating to any incident – always report to SLT/ DSL pending the nature of the post
- Reporting any incident to the appropriate member of staff immediately.
- Keeping any evidence of an incident. If they need help from a technical point of view – the Head of ICT or our network providers would be able to offer advice

Getting offensive content taken down

If online content is offensive or inappropriate, and the person or people responsible are known, staff need to ensure that those responsible understand why the material is unacceptable or offensive and request they remove it. Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report.

Remember - some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

Before you contact a service provider, it is important to be clear about where the content is; for example by taking a screen shot of the material that includes the web address. If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions. Where the material is suspected of being illegal the school will contact the police directly.

What to do with a report of cyberbullying?

Against a pupil……? Save all the evidence (screen shot etc) Is the pupil/student at risk?

NO? Report to form tutor Investigate and record on pastoral record. Internal sanctions

YES? Report to the DSL. Investigate. Use outside agencies/police

Against a member of staff……? Save all the evidence (screen shot etc). Report to line manager SLT/DSL. Investigate. Contact online safety helpline (www.saferinternet.org.uk) and/or social media site. DSL will help decide if further action is necessary involving police

Reporting Cyberbullying

Where appropriate, we will contact the police, the local CSCP or other outside agencies.

If the bully is a member of the school community:

- We will work with and take steps to change the attitude and behaviour of the bully.
- The school will take care to make an informed evaluation of the severity of the incident,
- The school will deliver appropriate and consistent sanctions. (see anti bullying/behaviour and sanctions policy)

Useful resources:

The Professional Online Safety Helpline
http://www.saferinternet.org.uk/ 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.

The DFE also promotes advice found at CEOP's Thinkuknow website www.thinkuknow.co.uk

Parent Zone has established a training programme designed to enable schools and professionals working with parents to deliver their own sessions on internet safety. They also provide innovative resources for schools to help and support parents, particularly around e-safety.

Parents at HH are regularly informed by newsletter should a safeguarding alert be prevalent. Digital parenting is also a resource that we use – a magazine that provides up to date advice for parents. Useful websites are also highlighted on occasion in our newsletter

Facebook has produced Empowering Educators support sheet specifically for teachers and launched the Bullying Prevention Hub with Yale's Centre for Emotional Intelligence.

Contact details for reporting issues on social networking sites

ask.fm	http://www.saferinternet.org.uk/safety-tools/askfm
Disney CLUB PENGUIN	http://www.saferinternet.org.uk/safety-tools/Disney-Club-Penguin
facebook	http://www.saferinternet.org.uk/safety-tools/facebook
flickr	http://www.saferinternet.org.uk/safety-tools/flickr

Google+	http://www.saferinternet.org.uk/safety-tools/google
Insta	http://www.saferinternet.org.uk/safety-tools/instagram
moshi monsters	http://www.saferinternet.org.uk/safety-tools/moshi-monsters
MOVIESTAR PLANET	http://www.saferinternet.org.uk/safety-tools/moviestarplanet
Snapchat	https://support.snapchat.com/
tumblr.	http://www.saferinternet.org.uk/safety-tools/tumblr
	http://www.saferinternet.org.uk/safety-tools/twitter
Vine	https://support.twitter.com/forms/vine
YouTube	http://www.saferinternet.org.uk/safety-tools/youtube

And finally……The Checklist

Due to the rapidly changing technology which enables cyberbullying, the following checklist will be used regularly by HH:

- Our DSLs, school governors, and all school staff will keep up to date as possible with the Government's latest safeguarding advice. Specific cyberbullying information can be found at:

  www.digizen.org/cyberbullying and at
  www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying

- The whole-school community will be regularly reminded through ICT lessons/PSHE/Form time and assemblies to understand what is meant by 'cyberbullying', its potential impact, how it differs from other forms of bullying and why it is unacceptable.

- All staff will have professional development opportunities regarding understanding, preventing and responding to cyberbullying. Emphasis has been placed on the importance of understanding child protection and other legal issues that may relate to cyberbullying incidents.

- Current school policy, guidance and information relevant to cyberbullying is reviewed regularly, to ensure that it meets the needs of pupils and staff. This includes behavioural agreements: Acceptable Electronic Use Policies, Staff Code of Practice policies which include the use of mobile phones and cameras within school

- The whole-school community is reminded of the reporting routes and responsibilities of all members of the community

- Learning strategies and targets, as well as staff development programmes, support the innovative and engaging use of technologies and promote its positive use which modelling safe and effective practice.

- The impact of prevention and response policies and practice is monitored annually. Staff, pupils and parents should feel confident that we effectively support those who are cyberbullied.

This policy is reviewed annually along with other safeguarding policies unless circumstances* deem that this should be reviewed earlier.

Due to the previous global pandemic and the potential to move to online learning during another outbreak, an additional section has been added to our child protection policy including the increased vulnerability of pupils having to access teaching online more regularly and the impact this can have on all children's mental health and the increased vulnerability of those groups who have protected characteristics.

APPENDIX – Electronic user agreement :

Electronic Device Acceptable Use Agreement (Staff and Visitors) Sept 2022

Please read the following carefully.

It should be read in conjunction with the HH Staff Code of Practice Policy, KCSIE 2022, WTTSC 2018 (2020)

Application: This agreement is for all school staff including supply staff, governors, volunteers and long term contractors.

Access to ICT (mobile devices, mobile phones, computers, e-mail and internet) at Hunter Hall School is conditional upon proper use of these media and may be withdrawn, either temporarily or permanently, if the standards expected by the school are not upheld. I understand my agreement to make acceptable use of ICT facilities whist I am at Hunter Hall School extends to the use of ICT **both** when I am at the school and working from home on matters related to school. I understand the school has a legal obligation to safeguard all users of the ICT system and all members of the school community.

I understand that my access to ICT at Hunter Hall School may be compromised if I do not act in accordance with this Acceptable Use Agreement and that breaking of this agreement could result in confiscation of equipment and removal of access rights to the school's ICT system. Serious violations of this agreement may be referred to senior management and will result in disciplinary action.

As a condition of use of ICT at Hunter Hall School I undertake:

- not to disclose to anyone the password or login name associated with my use of IT resources; this includes not using accounts or passwords of others when making use of any form of ICT;
- not to cause any physical damage or engage in activities which could damage or corrupt the schools computers, computer systems or computer networks. This includes: hacking into other users folders, work or files, or the school's system;
- not to upload, send, access, store or display, offensive messages or pictures, or material that would cause offence. This includes any threatening or annoying language, or any language which might incite hatred against any ethnic, religious or other minority groups. Libellous comments about pupils, school staff, or visitors falls into this category, as does material which draw improper attention to the appearance or character of all those who work or visit the school;
- not to take any images or videos of pupils/children/staff without prior consent from the school or parent;

- not to engage in any form of cyber-bullying or inappropriate texting, I understand that cyber-bullying is a 'method' that includes unpleasantness via, for example, text message, instant-messenger services and social network sites, e-mail, and images or videos posted on the internet or spread via mobile phone (this is not an exhaustive list). It can take the form of any of the previously discussed types of bullying, i.e. technology can be used to bully for reasons of race, religion, sexuality, disability etc. Individuals engaging in this type of behaviour should expect to be dealt with under the school's discipline policies;
- not to view, share or upload or forward data communications sent in error on the school's e-mail system and to advise the sender that they have received it in error;
- be aware of GDPR when copying recipients into e mail correspondence – BCC being the tool to use for multiple e mail recipients

- not to view, upload or download any material that is unsuitable for the workplace; this includes material of a violent, dangerous or explicitly sexual nature, and material dealing with controlled substances or other illegal activities;
- not to create, transmit or cause to be transmitted any material about any individual, organisation or product without having taken reasonable steps to verify its accuracy;
- not to create, transmit or cause to be transmitted any knowingly defamatory material, including opinions expressed about an individual, organisation or product;
- not to create, transmit or cause to be transmitted material such as the copyright of another person;
- not to upload, download or open any files unless virus scanned, upload or transmit any Virus, Worm, Trojan Horse, Malware, Ransomware or any other similar form of program or coding whether executable or otherwise;
- not to create, transmit or cause to be transmitted any material which is unlawful; or gain deliberate unauthorised access to facilities or services accessible via local or national networks or world wide web;
- not to transmit by e-mail any confidential information of the school, including information relating to pupils, parents or employees of the school, other than in the normal course of your duties;
- not to gain unauthorised access to, or violate the privacy of, other peoples files, corrupt or destroy other people's data or disrupt the work of other people;
- not to disclose passwords to third parties without the consent of the school;
- not to send any message purporting to be someone else;
- not to transmit, or cause to be transmitted any repetitive e-mails to bulk receipts (spamming) save in the course of your duties;
- not to copy software – it is illegal. Those who do are liable to prosecution;
- not to bring the school into disrepute by any behaviour or action associated with the use of ICT during working hours or otherwise;
- not to use the technology that would facilitate access to the internet by means other than through the school's ICT system. This includes circumventing the school's systems by using proxy spinners to access forbidden or time controlled sites to access a personal internet connection;
- to respect copyrights and trademarks;
- to be aware that activity on the school network, including e-mail, the internet and social networking (including twitter and facebook) can be seen and is monitored;
- to be aware of software installed including SENSO on all school machines and also when accessing school through personal devices such as TEAMS teaching and the use of one drive
- to be respectful and appropriate when communicating using ICT such as social networking sites. This also includes the uploading or images and/or videos relating to colleagues, pupils and the school;
- not to add parents, carers, or children as friends or personal contacts on social media;
- not to engage in any discussion on-line outside of formal channels;
- to log off when my work has been completed;

- to report to the Head teacher any incident or activity in breach of these undertakings; to inform if I see, hear or read anything that makes me feel uncomfortable while using the Internet and e-mail;
- to understand where staff have been allocated a school owned device they will be liable for loss or damage due to negligence or inappropriate use;
- to understand that any personal electronic devices which I bring into school will be for my personal use and the following restrictions apply:

- to accept personal responsibility for any equipment which I bring into school and ensure that it is stored securely;
- to have current and up to date antivirus protection and firewalls on any device connected to the school network.
- to not have use of personal mobile devices within the classroom, have in sight on desks or whilst on duty. Personal mobile devices should only be used when not in a teaching or supervisory capacity and not in public teaching areas. (see below)

Acceptable Use Policy for mobile phones

Application: staff, catering staff, support staff and peripatetic teachers (the list is not exhaustive), guidelines and instruction for the appropriate us of mobile phones during school hours.

As a condition of my use of ICT at Hunter Hall School, I understand and undertake the following:

- staff are permitted to have their personal devices (mobile phones) about their person, however there is a clear expectation that **all** personal use is limited to allocated lunch and/or breaks and in designated areas – e.g. staffroom and staff studies;
- to have any mobile device switched off during lessons, to ensure that mobile devices do not disrupt classroom lessons with ringtones, bleeping or music;
- unless permission is granted personal mobile devices will **not** be used to make calls, send SMS messages, surf the internet, take photos or use any other application during school time and other educational activities, school mobile devices are available for such tasks;
- staff are not permitted to use personal devices for taking, recording or sharing images or videos of pupils; photographs and video recordings for use on school systems unless agreed by the HT. This must be undertaken only by a school secured device;
- to observe mobile free areas at all times;
- to ensure that the Bluetooth function of a mobile device is switched off at all times and not used to send images or files to other mobile phones;
- to turn mobile devices to silent or off during meetings;
- during school trips and sporting events, members of staff are permitted to use their phones or devices unobtrusively to enable them to contact the school and for school to be able to contact them, should they need to in an emergency, however wherever possible the school mobile should be used;
- EYFS : school staff are permitted to carry school owned mobile devices in the Early Years Foundation Stage (EYFS). However, all other mobile devices should be kept out of sight when visiting EYFS unless the user has the express permission of the Head of EYFS to use it onsite;
- EYFS - all personal mobile devices should be kept in an allocated area in the Nursery and Reception during the school day;
- EYFS to only use personal devices if permission has been sought from the EFYS Leader;

- EYFS, in exceptional circumstances there may be the need to have a personal mobile device turned on and accessible during the school day. In this case, the Head teacher and EYFS leader must be notified;

- visiting adults who may need to use personal devices are under the responsibility of the particular host. It is their responsibility to convey the rules and regulations governing such devices;
- mobile devices that are found on-site and whose owner cannot be located should be handed into the School Office;
- the school accepts no responsibility for replacing lost, stolen or damaged mobile devices.

Monitoring

The school, as with all schools, is in a special position because of its obligation to promote and safeguard the welfare of its children, establishment and staff. Accordingly staff should not have any expectation of privacy in their use of the schools ICT systems.

I understand that the school regularly monitors the use of the Internet, social media, e-mail and school systems to check that it is being used in accordance with the school policies. The monitoring of these systems may be random or in response to a particular concern.

For example:

- to help the school with its day to day operations. i.e. if a member of staff is on holiday or sick, their e-mail account may be monitored in case any urgent e-mails are received;
- to check staff compliance with policies and procedures and to help the school fulfil its safeguarding legal obligations. i.e. to investigate an allegation of a staff member sending abusive text messages.

If it is discovered that any of the systems are being abused and / or the terms of this agreement are being infringed, I understand that disciplinary action may be taken which could result in dismissal.

I have read and understood these rules and asked for further clarification if unsure as to my obligations:

Name ----------

Signed ----------

Date ----------
