E-Safety Policy

Hill View Primary Academy

Version: 5	Date: September 2021
Approved by Board of Governors:	Date: October 2021
Next Review Date:	September 2022
Written by:	Deputy Head

Updated with reference to KCSIE 2021

Contents

.

Learning and Teaching

At Hill View Primary Academy, we believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

1. Aims

Our school aims to:

- deliver an effective approach to the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today and tomorrows digital world.
- recognise that online digital behaviour, including social media activity, must be upheld beyond the confines of the school gates and school day, and regardless of device or platform to ensure the online safety of our community including but not limited to pupils, staff, volunteers, visitors, parents, carers and governors.
- help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world.
- establish clear mechanisms to identify, intervene and escalate online misdemeanor with robust processes to follow where there are doubts or concerns.
- protect pupils from the risks associated with using devices connected to the internet whilst accessing remote learning.

In addition we are mindful that our overriding aim is to ensure children are kept safe and taught to keep themselves safe whilst online or using digital devices. In KCSIE 2021 it states:

> *24. All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.*
>
> *25. In all cases, if staff are unsure, they should always speak to the designated safeguarding lead (or deputy).*

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2021, and its advice for schools:

- Teaching online safety in schools 2019
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Linda Hamlyn (Safeguarding Governor)

All governors will:

- ensure that they have read and understand this policy
- monitor the implementation of the policy
- agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Senior Leadership Team

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- All member of SLT should ensure the policy is regularly monitored and report to the governing body on its implementation and regular updating of procedures.
- Will designate from within SLT an Online Safety leader with the roles set out below.
- Will ensure that all members of the school have appropriate e-safety training.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the school, in particular the DSL will:

- be fully aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer.
- support the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- ensure the governing body are kept informed of all online safety issues.

- ensure that any online safety incidents or incidents of cyber- bullying are logged (see appendix 5) and dealt with appropriately in line with this policy and the school behaviour policy.
- liaise with other agencies and/or external services if necessary.
- ensure that all staff have received suitable training and at least one member of staff has received recognised certification in dealing with online safety (such as the CEOP Ambassador or NSPCC Keeping Children Safe Online schemes) and is available to offer advice and train other staff where necessary. (appendix 4 contains a self-audit for staff on online safety training needs)

This list is not intended to be exhaustive.

3.4 The e-Safety Lead

The e-Safety lead is responsible for:

- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- establishing and reviewing the online safety policies / documents.
- offering advice and support for all users.
- keeping up to date with developments in online safety.
- understanding and knowing where to obtain additional support and where to report issues.
- liaising with national and local association as relevant.
- receiving reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- monitoring incident logs.
- reporting regularly to the Safeguarding Leader.

3.5 The ICT Technician/Lead

The ICT manager is responsible for:

- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- create systems that enable the school to monitor online safety related to school equipment and its online presence and conduct a full security check of the school's ICT systems on a regular basis.
- monitor the appropriate use of ICT resources used by students on a daily basis.
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- reporting issues to the e-Safety Officer.

- supporting the DSL in providing training for all staff.

The ICT Lead is responsible for:

- supporting e-safety policies by ensuring that e-safety is taught effectively within the curriculum for all year groups.
- supporting the DSL in developing educational materials for students which can be delivered outside of the curriculum.

This list is not intended to be exhaustive.

3.6 All staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an up-to-date awareness of the school's current online safety policy and practices.
- implementing this policy consistently.
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- to ensure that any suspected misuse or problems are reported to the DSL – particularly where it is believed that a child's welfare is at risk.
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- use digital communications with children and young people on a professional level and where possible only carried out using the official systems of the group.
- ensure young people in their care are aware of online safety.
- be aware of online safety issues particularly those related to the use of mobile phones, cameras, gaming consoles and handheld devices and that they monitor their use and implement the group policies with regard to these devices.

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- ensure that their children understand the need to use the internet and mobile devices in an appropriate way.
- notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- sign the relevant permission forms on the taking and use of digital and video images.
- ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

4. Educating pupils about online safety.

The children_are responsible for using Hill View's digital technology systems in accordance with the Pupil Acceptable Use Agreement. Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- demonstrate positive online behaviour.
- use technology safely and respectfully, keeping personal information private.
- understand that anyone they do not know in real-life is a stranger and that talking to strangers online can be dangerous.
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- use technology safely, respectfully and responsibly.
- recognise acceptable and unacceptable behaviour.
- develop a deeper understanding of the digital world in which they are growing up.

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.*
- *How information and data is shared and used online.*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.*

- *How social media works on a business level (that is not free and that it is paid for by the data of its users) and how big technology companies use various tricks to affect our online behaviour and the amount of time we spend using our devices.*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies and dedicated lessons by a specialist ICT teacher to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating Parents about Online Safety

The school will provide online safety information to parents and carers through:

- Letters, newsletters, web site, workshops.
- Meetings with parents / carers (formal and informal).
- Sharing the group's policies with parents and carers.
- Engaging parents in the signing of acceptable usage policies.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyberbullying

Definition

Cyberbullying is bullying using technology to threaten, embarrass or cause discomfort. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy).

Seven categories of cyberbullying have been identified:

- **Text message** bullying involves sending unwelcome texts.
- **Picture/video-clip** bullying via mobile phone cameras with images or video clips usually sent to other people.
- **Phone call bullying** via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible.
- **Email bullying** often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming**, Chat room and Social Networking Site abuse involves sending menacing or upsetting responses to pupils or young people.

- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

6.2 Preventing and addressing cyber-bullying.

The school will:

- ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- 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. The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.
- support parents in this are by sending information/leaflets on cyberbullying so that parents are aware of the signs of cyberbullying, how to report it and how they can support children who may be affected.
- ensure that all staff are aware of the Prevent Duties.
- provide training 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. (see section 11 for more detail).
- 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.

6.3 Guidance for Pupils about cyberbullying

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.

6.4 Guidance for Parents and Carers about cyberbullying

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 cyberbullying.
- Parents/carers should also explain to their children legal issues relating to cyber-bullying.
- If parents/carers believe their child is the victim of cyberbullying, 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.
- 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.

6.5 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1-3). The Acceptable Use register will be kept in the main office and updated by the Office Manager. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

7.2 Pupils Publishing Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff. If children have their own Scratch account, they must seek the permission of the teacher before they sign in and they must sign out at the end of the lesson. Pupils are not allowed to share Scratch projects or communicate with other Scratch users using school equipment.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use portable devices to store images/video/sound clips of pupils.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8 Email

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

- Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.
- Staff should not send emails to pupils.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails.
- Irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply.
- Chain messages are not permitted or forwarded on to other school owned email addresses.

9 Mobile Phones and Devices in School

General use of personal devices on school grounds

- No images or videos will be taken on mobile phones or personally owned devices.
- In the case of school productions, Parents/Carers are permitted to take pictures of their child in accordance with school protocols which strongly advise against the publication of such photographs on social networking sites.
- The sending of abusive or inappropriate text, picture or video message is forbidden.
- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity.
- Mobile phones and personally owned devices such as Smart Watches will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Mobile phones or devices can only be used during designated break times away from the children.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

9.2 Pupils' use of personal devices

- Pupils' who need to bring a mobile phone in to school will check their device into the School Office at the beginning of day and pick up prior to leaving at home time.
- Pupils must ensure that their mobile phones are fully turned off when they hand them into the School Office.
- Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.
- Pupils are not permitted to use their devices to attempt to communicate with school staff or governors.
- Pupils are not allowed to wear a 'smart' watch, or any watch that has the same functionality as a mobile phone or PC, on the school site.

10. Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers).
- All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the DSL.
- All communication between staff and members of the school community on school business will take place via official approved communication channels.
- Any communication from students/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools' policies and the wider professional and legal framework.
- Members of staff will notify the DSL immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- Members of staff are encouraged not to identify themselves as employees of Hillview Primary Academy on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

11. Staff using work Devices outside School

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

- Work laptops which are taken home should be encrypted.
- USB devices containing data relating to the school must **not** be used – all teachers are able to use remote access and save to the server. Teachers should **not** save to their laptop.
- If staff have any concerns over the security of their device, they must seek advice from the IT Technician.
- Work devices must be used solely for work activities.

12. Authorising Internet Access

- All staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources.
- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- All visitors and students will be asked to read and sign the Acceptable User Policy prior to being given internet access within the school.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- The school will maintain a current record of all visitors who have been granted 'Guest' access to the school's internet provision.

13. How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. (See appendix 1)

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Training

All new staff members will receive training from the Designated Safeguarding Lead (DSL), as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

15. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every two years by the Headteacher. At every review, the policy will be shared with the governing board.

16. General Data, Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding to all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.
Personal and sensitive information should only be sent by e mail when on a secure network.
Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the Trust's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO). Their details are: Ian Arkell, SchoolPro TLC (Arkell@schoolpro.uk)

17. Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the DSL). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

18. Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as ‘sexting’; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children’s Social Care may be notified.

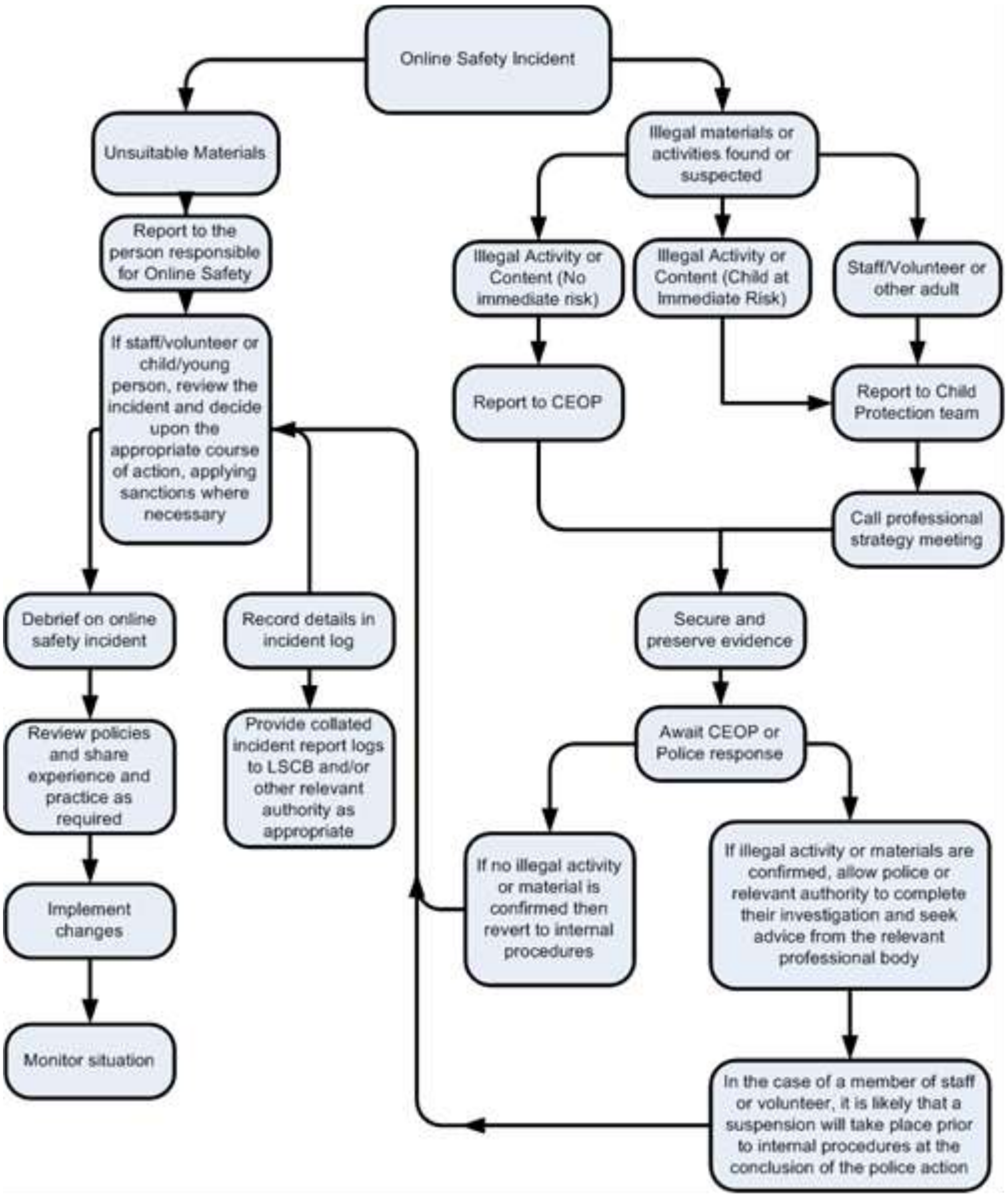
Our school follows and adheres to the national guidance - UKCCIS: *Sexting in schools and colleges: Responding to incidents and safeguarding young people*

19. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child Protection policy
- Remote Learning Policy
- Behaviour policy
- Anti-Bullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1 – Response to issue of misuse


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 2

Staff, Governors, Student and Volunteer Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for students/volunteers to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that all adults will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that all adults are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that adults will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect students/volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the Hill View Primary Academy will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *Hill View Primary Academy's* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Hill View Primary Academy:

- When I use my mobile devices (laptops / tablets / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I
will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems without seeking permission.
- I will not use USB devices whilst at the school.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programs). If I believe that a link or attachment may be malicious, I will report it to the school leadership team, so that the rest of the staff and governors can be warned about it.
- I will ensure that my data is regularly backed up, in accordance with relevant school / policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not try to use any program or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine , or store programs on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School GDPR Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
  - Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school*:*

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the trust/university and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ....

Position in school: ....

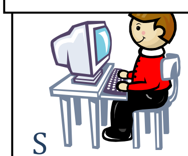
Signed: ....

Date ....

Appendix 3 - EYFS and KS1 acceptable use agreement (pupils and parents/carers)

<u>Our School e-Safety Agreement</u>

EYFS/KS1: Think before you click!



S

I will only use computers and the Internet with an adult in the room

A

I will only click on icons and links when I know they are safe

F

I will only say kind things online

E

If I see something I don’t like on a screen, I will always tell an adult

My Name:

My Signature:

For Parents:

EYFS/Key Stage 1: All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent's Consent for use of technology:

Computing, Internet and ICT: As the parent or legal guardian of the pupil named overleaf, I grant permission for the school to give my child access to:

- the Internet at school
- the school's chosen email system

(They can only send/ receive @hillview.bournemouth.sch.uk addresses)

- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

Mobile and wearable technology that can connect to the Internet is not allowed in school for Safeguarding and other reasons. Under exceptional circumstances certain wearable technology may be permitted but parent/ carers will need to sign a separate form to confirm that such technology meets the Safeguarding expectations of the school.

My child's name: ____________________________________

Parent / guardian signature: ____________________________ Date: ___/___/___

Appendix 4 - KS2 acceptable use agreement (pupils and parents/carers)

Our School e-Safety Agreement

KS2: Think before you click or tap!

These rules will keep me safe and help me to be fair and respectful to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit websites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything that I am unhappy with or I receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult.
- I will handle and carry equipment carefully, the way my teacher shows me.

Mobile and wearable technology that can connect to the Internet is not allowed in school for Safeguarding and other reasons. Under exceptional circumstances certain wearable technology may be permitted but parent/ carers will need to sign a separate form to confirm that such technology meets the Safeguarding expectations of the school.

I have read and understand these rules and agree to them.

Signed:____________________ **Date:** ______________

Pupil:_______________ **Class:** ______________

For Parents:
Key Stage 2: All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent's Consent for use of technology:
Computing, Internet and ICT: As the parent or legal guardian of the pupil named overleaf, I grant permission for the school to give my child access to:

- the Internet at school
- the school's chosen email system

(They can only send/ receive @hillview.bournemouth addresses)

- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.
Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.
I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.
I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.
I will not take and then share online, photographs of other children (or staff) at school events without permission.
Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.
I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.
I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

Mobile and wearable technology that can connect to the Internet is not allowed in school for Safeguarding and other reasons. Under exceptional circumstances certain wearable technology may be permitted but parent/ carers will need to sign a separate form to confirm that such technology meets the Safeguarding expectations of the school.

My child's name: ______________________________________

Parent / guardian signature: _____________________________ Date: ___/___/___

Appendix 5

Wearable technology acceptable use agreement.

Wearable technology is not permitted in school, without express consent from the school, for reasons of Safeguarding and supervision.

In addition:

- Most management accounts and apps for wearable technology are linked to mobile phones and user agreements, usually with a minimum age of 12/13. The use of Mobile Phones and associated technology that does not belong to the school is not permitted by pupils during school time.[1]
- Devices may become a needless distraction from learning.
- Devices often have considerable value and the school cannot be responsible or held liable for damage or theft should they be worn to school.
- The school cannot be responsible for determining which wearable devices can connect to the Internet to send and receive digital messages or potentially upload media. Safe supervision therefore necessitates that no wearable device is permitted.[2]

The approach taken by the school is that should smart, electronic or wearable devices come to school they may be confiscated, parents contacted and held by the school to be returned home.

In exceptional circumstances, some wearable technology (e.g. Fitbits etc) **may** be permitted, providing they meet the thresholds for Safeguarding and cannot connect wirelessly to the internet during school hours. Decisions will be made on a case-by-case basis and parents will be expected to agree, sign and comply with the User Agreement below.

Hill View Wearable Device Consent and Acceptable User Agreement.

Child's name:________________________ __________Year___________ Class____________

I can confirm that my child's wearable device:

- Complies with the thresholds for safeguarding and supervision at the Academy;
- Is not a true smart device (capable to downloading and running apps), merely a fitness tracker (such as a basic Fitbit type device).
- Is not able to wirelessly connect to the internet during school hours without the use of a connected phone.
- Is not capable of recording or playing media (including sound, photographs or video recordings) of any description, nor is it capable of downloading or uploading any text, sound or media to the Internet or any mobile network;
- Has no age recommendations related to it, or any software linked to it, that state that the user should be older than my child.

I understand that the school can take no responsibility for loss or damage of a wearable device and that misuse by my child will result in the device being confiscated and sent home.

This consent may be withdrawn by the school at any time.

I agree to the terms and to comply with this agreement:

Signed_____________________________________ Date:_____________________

Print name______________________________________

Approved: ____ Date:______________

Role:____________________________

[1] (For example, in relation to Fitbit, 'persons under the **age** of 13, or any higher minimum **age** in the jurisdiction where that person resides, are not permitted to access or **use** the **Fitbit** Service unless their parent has consented in accordance with applicable law'.)

[2] The exception to this is related to devices to support Health Care Plans or reasonable adjustments as defined in the equality act.

Appendix 6 – Online Safety Training Needs Audit

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	