Online safety policy

Hill View Primary Academy

Version 8	October 2023	
Approved by:	Governors	**Date:** November 2023
Last reviewed on:	October 2023	
Next review due by:	October 2024	

Table of 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:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- 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 DfE'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 that we deliver predominantly through Purple Mash.

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems.
- Reviewing filtering and monitoring provisions at least annually.
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning.
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Hannah Staddon (Safeguarding Governor).

All governors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

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

The DDSL team, including DDSL for Online Safety, takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

The DDSL for Online Safety will work with the Computing Teacher that predominantly delivers the Computing curriculum.

3.4 The ICT technician manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- 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)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by Hill View Primary Academy.
- Following the correct procedures by Hill View Primary Academy if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- 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/carers 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 resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Online safety is embedded throughout the curriculum however it is particularly addressed in the following subjects:

- Computing
- RSE
- PSHE

The curriculum and the school's approach to online safety is developed in line with the DfE's 'Teaching online safety in school' guidance and the associated UK Council for Child and Internet safety's 'Education for a connected world framework.'

We use the Purple Mash Computing Scheme of Work Online Safety units to teach many aspects of online safety within the context of Computing as a subject. This aims to give pupils the underpinning knowledge of aspects of the online world to help them develop behaviours that can navigate safely and confidently regardless of the device platform or app they're using. It also aims to help pupils develop appropriate scepticism and reasoning when they encounter new online experiences to be able to evaluate the risks or potential pitfalls of these encounters.

We further reinforce and expand this teaching through the PSHE and RSE curricula which also cover aspects of online safety.

We supplement this teaching with whole school online safety awareness, specialist visiting speakers, for example, the Coram Life Bus, and through role modelling in the day-to-day life of the school.

Online safety teaching is appropriate to pupil's ages and developmental stages as well as being flexible enough to be tailored to any specific emerging threat within the community.

The underpinning knowledge and behaviours pupil learn through the curriculum include the following:

- Evaluating what they see online.
- Recognising techniques used for persuasion.
- Clear understanding of acceptable an unacceptable online behaviour.
- Identifying online risks.
- How to seek support.

External resources are reviewed by teachers prior to using them for the online safety curriculum to ensure that they are appropriate and to ensure that they are valid sources of information based upon evidence and of high quality. When external visitors are invited into school to deliver certain aspects of the online safety curriculum the head teacher and DSL team ensure that the visitors selected are appropriate. Before conducting a lesson or activity on online safety the class teacher and DSL team consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL team advises staff members on how best to support any people who may be especially impacted by lesson or activity. Lessons and activities are planned so they do not draw attention to individual pupils who may be experiencing difficult circumstances. If a staff member is concerned about anything pupils raise, they will make a report in line with the safeguarding policy.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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

- Use technology safely and respectfully, keeping personal information private.
- 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 (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

We also teach about:

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Inclusion.

We aim to enable all pupils to have a thorough understanding of how to protect their own and others' safety online. This includes children of all abilities, social and cultural backgrounds, those with SEND and EAL speakers. We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day and in some cases beyond the school day.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less a comprehensive support network from family and friends in staying safe online e.g. pupils with SEND and LAC. Relevant members of staff e.g. the SENCO and designated teacher for LAC work together to ensure the curriculum is tailored so these pupils receive the support that they need.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or connected or recommended third party virtual learning environment (VLE). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

6. Cyber-bullying

6.1 Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We 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.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. The Computing Teacher, Class Teachers, SLT and other members of staff will discuss cyber-bullying with their classes or year groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL team will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices.

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence?

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a member of SLT.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil’s co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a ‘good reason’ to do so.

When deciding whether there is a ‘good reason’ to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with a designated member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Hill View Primary Academy recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Hill View Primary Academy will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Hill View Primary Academy.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Any school or tutor group time
- Clubs before or after school, or any other activities organised by the school.
  - 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.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices

General use of personal devices on school grounds or whilst supervising pupils away from the school site.

Staff are not to use their own mobile devices or technology except in designated staff areas, away from the pupils and/ or at times when pupils are not present in the building. Exceptions to this may include those staff such as SLT that may need to do so as part of their role or staff that have been given permission to do so, for example on a trip.

- 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 and visitors 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 (SLT may have occasional to do so but personal numbers will be blocked).
- 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.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school’s terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Head or Deputy Head Teacher.

10. 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 ICT and internet acceptable use –The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DDSL team 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 child protection and safeguarding policy.

12. Monitoring arrangements

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

This policy will be reviewed every year by the Online Safety lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

EYFS/KS1: Think before you

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

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

I will only say kind things online

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.

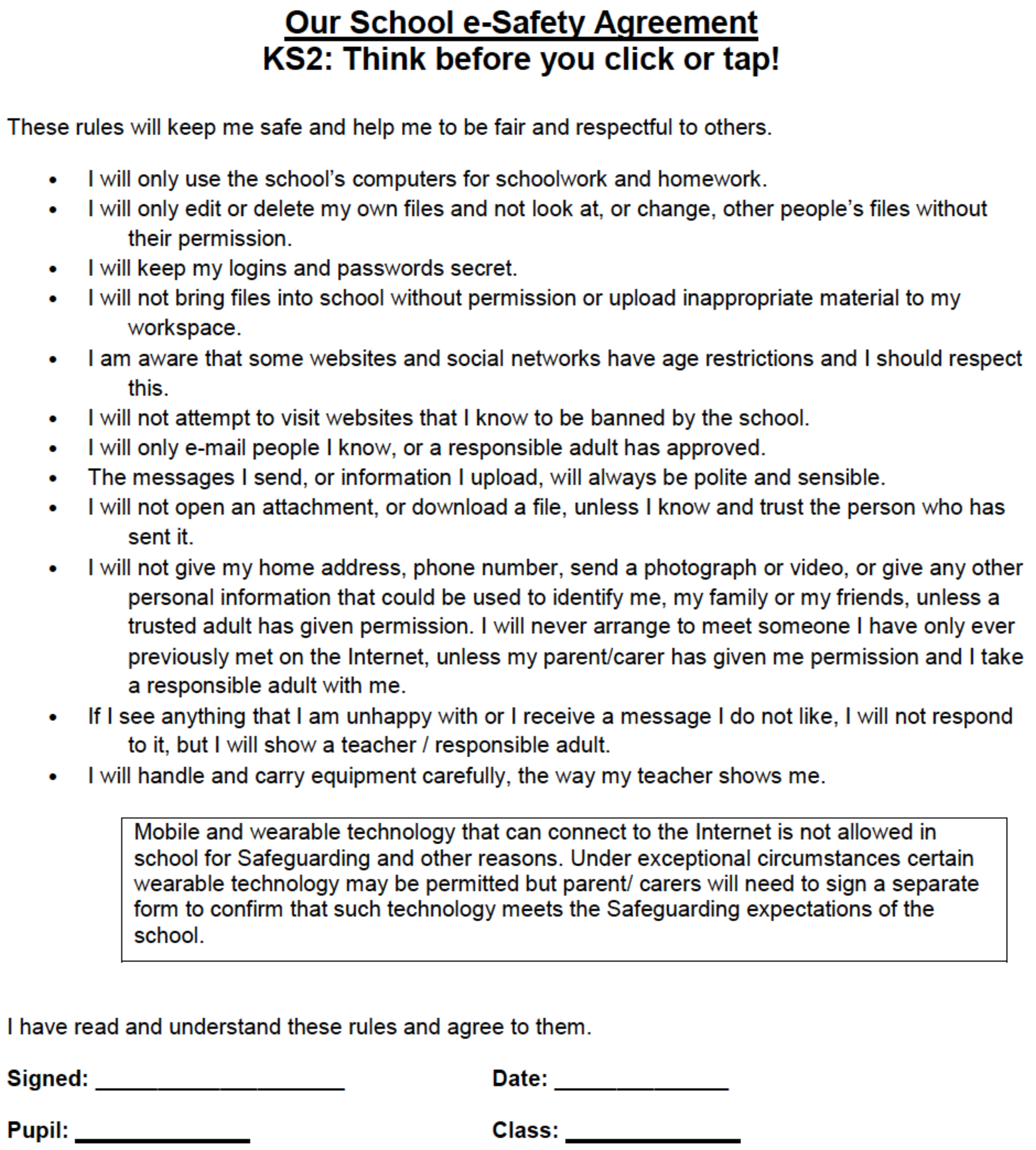
I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
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 2: 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.

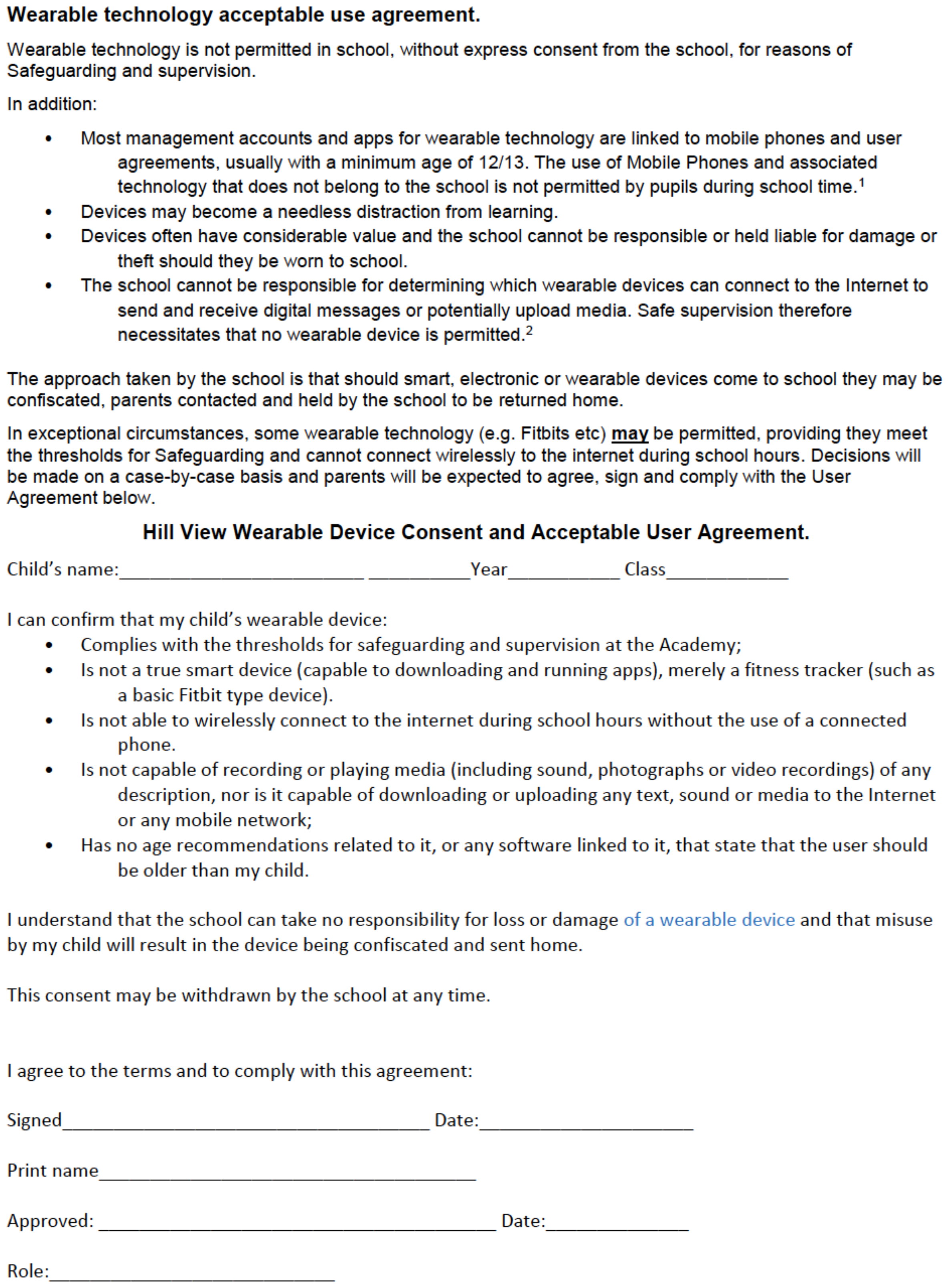
I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.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



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:_____________________________

Staff, Governors, Volunteers and visitors Acceptable Use

ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school’s reputation.
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software or connect unauthorised hardware or devices to the school’s network.
- Share my password with others or log in to the school’s network using someone else’s details.
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I’m not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school

I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school’s ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

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?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**