

Houghton on the Hill E-Safety Policy

Revised December 2023

Responsible Committee – Safeguarding



Rationale

At Houghton on the Hill Primary School we provide a computing curriculum designed to equip our pupils for an ever-changing technological world. We provide opportunities to develop children's ability to think critically and creatively as well as developing their computational thinking.

One of our main aims is to keep our pupils safe online. We provide them with the knowledge and skills to do so, promoting safe messages throughout the curriculum. Our Christian values link together with our teaching of E-safety; we teach the children how to show these values in the online world. We recognise that as a school we have a responsibility to prepare the pupils for their future by improving their knowledge of and understanding of how imperative technology is as an aid to learning and the real world beyond school.

Houghton School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information

- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Aims

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [preventing and tackling bullying](#) and [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.

E-Safety Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

The local governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

Headteacher:

The headteacher is responsible for:

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL, IT manager and Computing Coordinator to conduct light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy as required.

The DSLs and Computing Coordinator

The DSLs and Computing Coordinator are responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety.
- Working with the headteacher and governing board to update this policy. Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary

IT Manager/Technician

The IT Manager/Technician 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 IT 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 IT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Maintaining an understanding of this policy

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable the school's acceptable use policy
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately

Pupils

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns to a member of school staff.

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 IT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites: 5

- What are the issues? UK Safer Internet Centre: [What are the issues? - UK Safer Internet Centre](#)
- Hot topics, Childnet International: [Help & advice | Childnet](#)
- Parent advice, Childnet International: [Parents & carers | Childnet](#)

Visitors and members of the community who use the school's IT 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.

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience.

Educating pupils about online safety Pupils will be taught about online safety as part of the curriculum.

In Key Stage 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 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
- How to report a range of concerns

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home such as Class Dojo, and in information via our website. This policy will also be shared with parents.

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.

Acceptable use of the 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 and 2).

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

For further details refer to the staff Code of Conduct point 7.

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework and sharing ideas are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupil discover unsuitable sites, the URL, time and content shall be reported to the teacher who will then report the incident to the Headteacher, DSL, Computing Coordinator or IT technician. The URL will then be blocked on the school system.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work with its technical support provider to ensure filtering systems are effective as possible. We have in place web-filtering that blocks access to social media sites, chat rooms, online gaming sites and certain video hosting websites that do not have an internal filtering system.
- 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 and 2).
- 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.

Social Networking and EMAIL

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.
- Staff members must use the email address provided by the school for all school-related communication. Personal email addresses must not be used for school purposes and school emails must not be forwarded to a personal email account.
- School email accounts must not be used for any personal communication not related to school.
- School devices may not be used to access social networking sites for personal purposes on the school site but may be used to access and update the school's own social networking accounts.
- Staff, students and volunteers are reminded that social networking sites should be regarded as public forums and as such any discussion about school issues, colleagues or pupils is strongly discouraged. Any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school could result in disciplinary action.
- Staff members must make every effort to ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings on social media and must not disclose any confidential or sensitive information, or information or images that might compromise the security of the school.
- Staff members must not share personal information with a pupil (e.g. personal phone number or email address) or communicate with pupils via personal social networking accounts

Staff use of personal devices

- Staff members must not use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on school trips.
- All staff may use their mobile phones for the purposes of professional, work-related communication during school hours.
- Mobile phones must not be used for making personal phone calls, texting, checking personal emails or accessing personal social media sites in any teaching area in school during lesson times or while children are present.
- Mobile phones, iPads, iPods and any other portable devices must not be used in toilet or changing areas under any circumstances.

- Staff personal devices such as mobile phones, i-pads, cameras etc must not be used to take photographs of children.
- Where possible, all school related work should be carried out on a work device. In cases where a personal computer or laptop is used, staff must ensure that no personal or sensitive data are stored on that device.

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. These more advanced features may present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/ precaution use. These are handed to the class teacher on arrival to school and collected at the end of the day. 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.
- Staff should not use mobile phones to contact parents/guardians. School Staff will always use the school phone to contact parents/guardians.
- The sending of abusive or inappropriate text message is forbidden.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or on the playground.
- Staff may use their mobile phones for personal use in the staffroom during the lunch/playtime periods or before/after school.
- Parents cannot use mobile phones on school trips to take pictures of the children.

Digital/Video Cameras

Pictures, videos and sound are not directly connected to the internet but images are easily transferred.

- Pupils will not use digital cameras, mobile phones or video equipment as school unless specifically authorised by staff.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils' full names will not be used anywhere on a website, particularly in association with images.

- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The Headteacher or nominee will inform parents/carers and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

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 2.

Staff must ensure that their work device is secure, encrypted 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.

Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT manager.

Prevent Statement

The counter-terrorism and security bill was granted royal assent on 21 February 2015, which places a statutory duty on named organisations, including schools, to have due regard towards the need to prevent people being drawn into terrorism.

The most important part of this security bill is 'keeping pupils safe from the danger of radicalisation and extremism'.

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems used at Houghton Primary School block inappropriate content, including extremist content. Where staff or pupils find unlocked extremist content they must report it to the Headteacher, DSL or Computing Co-ordinator.

Cyber Bullying

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 one person or group by another person or group, where the relationship involves an imbalance of power.

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. Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies. 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.

The school also sends information/leaflets on cyber-bullying to parents so that 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 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.

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.

How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. 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 IT 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 and code of conduct.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Incidents which involve illegal activity or content will be reported to the police.

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, ebulletins and staff meetings). '

The DSL and deputies 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.

Copyright

Staff must ensure that they have permission to use the original work of others in their own or their pupils' work. Where work is protected by copyright (including music and videos), it must not be copied, downloaded or distributed without permission from the copyright holder.

Monitoring arrangements

Behaviour and safeguarding issues related to online safety will be logged on the school's online reporting system.

Links with other policies

This online safety policy is linked to:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Data Protection Policy
- Code of Conduct
- Anti-Bullying Policy

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

Acceptable use of the school's IT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's IT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school, I will leave it at the school office for safe-keeping and collect it at the end of the day.

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's IT systems and internet responsibly.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

I have read and agree to abide by the school's E-Safety Policy.

I will only use the school's IT 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.

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 IT 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 IT systems and internet responsibly, and ensure that pupils in my care do so too.

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

Date:

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
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 IT 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? Please record them here.	