

E-safety Policy

Hawthorn Primary School



Approved by:	Safeguarding
---------------------	--------------

Last reviewed on:	June 2025
--------------------------	-----------

Next review due by:	September 2026
----------------------------	----------------

Our Vision

We encourage children to become part of our 'Hawthorn Family' by providing an inclusive and creative environment enriched with experiences to nurture individuals socially, emotionally and academically enabling them to develop positive relationships. We support children to work together to achieve, succeed and become the best version of themselves.

Intent

At Hawthorn Primary School, E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety policy will operate in conjunction with other policies including those for Behaviour, Curriculum, Data Protection, Child Protection and Safeguarding.

End to End E-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Newcastle LA Network including the effective management of Websense filtering.
- National Education Network standards and specifications.

Writing and reviewing the E Safety policy

The E-Safety Policy relates to our safeguarding practices, as well as to other policies including those for Computing, Positive Behaviour and Wellbeing, Curriculum, Data Protection, Child Protection and Safeguarding.

The school has an E-Safety Coordinator. This will be the Designated Child Protection Coordinator and the Computing Coordinator and an Independent Data Protection Consultant, as the roles overlap.

Our E-Safety Policy has been written by the school, building on the government guidance. It has been agreed by all staff and approved by Governors. The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Internet use will enhance learning

Internet access will be designed for pupil use and will include filtering appropriate to the age of pupils. This is reviewed regularly. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. This is an integral part of their education from EYFS until they leave primary school. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

Staff will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. This is addressed through lessons and whole class discussions.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Newcastle LA.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

E-mail

- Pupils may only use approved e-mail accounts on the school system or a secure APP, e.g. Tocomail.
- Pupils must immediately tell a teacher if they receive an offensive e-mail and this will be addressed immediately.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. Children's names will be shown as initials only.
- The forwarding of chain letters is not permitted.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupil's work and photographs can only be published with the permission of the pupil and parents/guardians. Records are kept and updated regularly. E.g. A new admission in school.
- Pupils who are looked after by the Local Authority are published only at the discretion and permission of the authorised allocated social care officer.

Social networking and personal publishing

- We will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail address, full names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LA, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- The School use SENSO to ensure systems are in place to protect pupils and staff. This is monitored by the Head Teacher.
- If staff or pupils discover an unsuitable site, it must be reported to the Head Teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

We recognise that technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment which considers and reflects the risks our children face.

The Head Teacher will be informed of online safety concerns by the DSL and any staff who are made aware of online safeguarding concerns, as appropriate. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing board.

We will do all we reasonably can to limit children's exposure to online risks through school provided IT systems. We will ensure that appropriate filtering and monitoring systems are in place and are informed in part, by the risk assessment required by the Prevent Duty.

Managing mobile/wearable technologies

Wearable technology is any technology that is designed to be used while worn. Common types of wearable technology include smartwatches and smartglasses.

- **Staff** - If 'Wearable Technology' is worn in lessons or in public areas around the school, the 'Do not disturb'/'flight mode' should be activated.
- **Pupils** - Wearable Technology that has the ability to communicate, i.e. Camera, Microphone or message notifications, are not allowed to be worn in school. Pupils must seek permission from the school before wearing fitness tracking devices. If a Wearable Technology device is deemed by the teacher to be causing a distraction around school, it is liable to confiscation until the end of the school day.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR guidance of May 2018. See Data Protection policy for details.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. This is updated at the beginning of every academic year. New staff members will be given this document to sign before they begin their new post.
- We will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional supervised access to specific, approved on-line materials.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Newcastle LA can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a member of SLT.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and safeguarding policy.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to E-Safety (Police, NSPCC, Prevent Officer, Social Care, Local Authority)

Communications Policy

Introducing the E-Safety policy to pupils

- E-Safety rules will be posted in all classrooms and discussed with the pupils at the start of each academic year. It is also part of our wider curriculum. E.g. taught through digital literacy, PSHCE and Internet Safety Day.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school website. This is regularly updated.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key E-Safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images, including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.

Appendix 2: Internet Agreements Key Stage 1 and Key Stage 2

Key Stage 1 Internet Agreement

When using the Internet in schools I agree to do the following:

- I will ensure the children in Year _____ use the internet for activities set by myself.
- I will only allow children to use internet sites that I know or believe will help them with their learning.
- I will ensure that the children know that if they find any unpleasant or offensive material while searching the internet they will:
 1. Put the lid down on the lap top
 2. Quietly put up my hand to call for a member of staff who will make a note of the site

This agreement is designed to help you and the school and is part of the Hawthorn Primary School code of conduct.

I agree to what is written here.

Signed

Class teacher for Year _____

Date Signed.....

Key Stage 2 Internet Agreement

When using the Internet in schools I agree to do the following:

- I will only use the internet for activities authorised by my teacher.
- I will only go on internet sites that I know or believe will help them with my learning
- If I find any unpleasant or offensive material while searching the internet I will:
 1. Minimise the screen immediately
 2. Quietly put up my hand to call for a member of staff who will make a note of the site
 3. Exit the site and continue with my work.

This agreement is designed to help you and the school and is part of the Hawthorn Primary School code of conduct.

I agree to what is written here.

Signed

Year _____

Date Signed.....

Appendix 3: ICT Acceptable Use for Staff

Hawthorn Primary School ICT Acceptable Usage

- I have read and agree to abide by the Newcastle City Council ICT Information Security and Acceptable Use Policy Guidance for Staff.
- I will only use the school's Email / Internet / Intranet for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will ensure that personal data will be compliant with GDPR guidance and the Data Protection Policy (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the

parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will not have parents, pupils or ex pupils as direct friends on any social networking site I use e.g. Facebook. twitter etc.
- I will not make negative comments about school or colleagues on social network sites.
- I will be aware of my professional status when commenting on social networking sites.
- I understand that failure to comply with the Acceptable Usage Policy could lead to disciplinary action.

User Signature

I agree to abide by the above Acceptable Usage Agreement

Signature Date

Full Name(printed)

Job title

Appendix 4: Recommended sites for parents and children to access

<https://www.saferinternet.org.uk/>

<https://www.betterinternetforkids.eu>

<https://www.internetmatters.org>

<https://www.thinkuknow.co.uk/parents/>