

Amington Heath Primary and Nursery School



Online Safety Policy

Online Safety Coordinator- Paul Horton

**Policy approved: October 2026
Review due: October 2027**

Introduction

At Amington Heath Primary and Nursery School, we understand that online safety / online safety is not just about the safe use of the internet but all digital technology, systems, apps, online services, artificial intelligence tools and computing devices used within our school and wider community. We recognise the valuable contribution that the internet and digital computing devices can have on children's learning and can be a means of enhancing and engaging children in teaching and learning. We believe that the safe use of these technologies can be a beneficial teaching tool and aim to teach our children to use them responsibly, respectfully, critically and independently.

Aims

We aim to use an embedded and cross-curricular approach to teach our children:

- To ensure their personal information always remains safe and to never provide it over a digital platform including but not limited to social media, email, blogs, gaming and websites.
- To understand that pop ups can lead to viruses or inappropriate content and that they should close them or block them if they occur. In school pop up blockers are always activated on desktops, iMacs and ipads.
- That the internet should only be accessed in school with the permission of an adult and that if any inappropriate content appears that they should press the report button, minimise the screen and report the issue to a teacher immediately.
- That they should never arrange to meet someone in real life who they met in the online world unless arranged through a parent/carer.
- Children should not engage in communication online through websites or email without the presence or permission of a teacher.
- To communicate respectfully with others online and ensure that they do not say anything hurtful, racist or abusive to others. At Amington Heath, we treat others as we would like to be treated both in the real world and the digital world. Children are taught that emails must always be courteous and polite and our emailing system is monitored by teaching staff.
- Children know that they should not take photographs or upload any image without the person's permission.
- Children know that sites, games, videos and media have age ratings and why these ratings should be adhered to.
- Children are taught to recognise acceptable and unacceptable online behaviour and how these can impact on other users.
- To ensure that their digital presence is positive and that appropriate filters, privacy settings and virus protections are needed.
- To take responsibility for their actions when interacting with digital technology and the reporting of ICT and online issues.
- To use only teacher permitted search engines and links while in school and in the presence of a member of teaching staff.
- That they should not download any software or app without adult permission.
- That children understand online sexual harassment, cyberbullying, youth-produced sexual imagery, consensual and non-consensual image sharing, and AI-generated or manipulated images are safeguarding concerns and must be reported immediately.
- That children know how to question online information, check reliability, identify persuasive design, recognise misinformation/disinformation and seek trusted adult support when unsure.
- That children understand the additional risks linked to generative artificial intelligence, including inaccurate information, age-inappropriate responses, deepfakes, image manipulation, impersonation, data privacy risks and AI-assisted scams.

Teaching and learning

At Amington Heath, we acknowledge the internet is an integral part of 21st century living and the responsibility we have as educational practitioners to provide our children with an up to date safety

curriculum which equips them with the skills they need in order to remain safe online. We understand that part of our duty is to provide children with quality internet access through a variety of devices; including tablets and desktops as well as the ability to apply the learning to laptops, mobiles and gaming devices which they have in their homes.

The use of ICT and the internet is embedded throughout the curriculum to ensure pupils leave Amington Heath with a high level of digital literacy which they will be able to apply to technological advancements in the future. Similarly, we use each of these opportunities to reinforce our online safety school ethos and key messages which are described above in the aims section.

As a school, we have developed an internet safety progression ladder (Appendix 1) to ensure our children are receiving an age-appropriate curriculum in every phase and year group. These statements have been reviewed in line with the National Curriculum for Computing, statutory safeguarding guidance, DfE Teaching Online Safety in Schools guidance, RSHE expectations, KCSIE 2025 and the draft KCSIE 2026 consultation. The curriculum will continue to be reviewed by leaders, governors, pupils, parents.

We use the 4Cs of online risk - Content, Contact, Conduct and Commerce - when discussing safety with our children. This language supports a well-rounded safety curriculum which considers harmful material, unsafe communication, behaviour online, financial exploitation, scams, gambling-style features, advertising and in-app purchases.

We are committed at Amington Heath to safeguarding our children while providing an interactive, motivating and engaging curriculum which uses a wide range of resources including iPads, Apple TV, desktop all-in-one computers, Chromebooks, tablets, laptops, cameras, programmable devices and approved educational software. This policy has been written with reference to Keeping Children Safe in Education 2025, Working Together to Safeguard Children 2026, DfE filtering and monitoring standards, DfE cyber security standards and DfE guidance on generative AI in education. Draft KCSIE 2026 has also been considered ahead of implementation, subject to final publication.

Managing Internet access

School website

- The school website is edited by the Office Manager who ensures that copyright law, GDPR requirements, safeguarding expectations and photo-use permissions are followed. The website is managed by an external company with close links to school.
- The only contact information detailed on the website is that of the school site and office email. All other staff's information should not be published. The senco email address can be found on the SEN information report in-line with policy and best practice.
- While the Office Manager takes control of the editing of the site, the head teacher takes overall responsibility for checking its accuracy and appropriateness.
- The website was designed and edited in line with DfE statutory requirements.
- The website contains an online safety / online safety page which provides pupils, parents and the wider community with information on staying safe online, reporting concerns and accessing current support such as CEOP, UK Safer Internet Centre, NSPCC and Childline.
- Staff have access to edit their class pages however only once full training has been provided.
- Public-facing images and videos of pupils will be used only in line with parental consent, GDPR and safeguarding expectations. The school will avoid publishing pupils' full names alongside identifiable images and will periodically audit public images to reduce risks linked to misuse, AI manipulation and image-based abuse.

Email

- Pupils are only allowed to use school email addresses which are created as part of our learning platform and monitored by teaching staff.

- Pupils do not have individual email accounts but instead a class set of 30 email addresses have been created so that they can be used for the teaching of emails.
- Pupils are only allowed to email each other while a teacher is present and the outgoing and incoming messages are monitored by the class teacher, online safety co-ordinator and technician.
- Pupils are taught to use email respectfully and responsibly and are educated about the potential dangers of spam mail.

Learning platform

- We use Microsoft office 365 as our online learning platform where we have a dedicated staff and SLT site.
- Passwords must meet current school security requirements and should not be shared. Staff accounts must use multi-factor authentication where available, especially for email, cloud services, administration systems and remote access. Password resets, account access and leavers' accounts will be managed promptly by authorised staff or IT support.
- The staff site along with curriculum is only accessible to teaching staff and the SLT site is only accessible to members of SLT.
- Access to Microsoft 365, shared drives and safeguarding or pupil-data systems will be based on role and need. Leaders and IT support will review user access at least annually and when staff join, change role or leave.

Online resources for home learning

- Children have access to NumBots/Times Table RockStars, Morphs, Hairy Reading and Nessy at home. Each child has their own individual login and, while they can play against other children in the school and wider platform, communication features are disabled or restricted where possible. These platforms are monitored by relevant curriculum leaders and the headteacher/safeguarding team where appropriate.

Facebook

- The school operates a school Facebook page which is monitored and edited by assigned individuals in school. Only authorised staff are able to upload posts. All staff receive training in this and how to keep children safe in line with KCSIE and current school safeguarding expectations.
- Any content uploaded by school is subject to approval and our safeguarding and GDPR policy in line with the consent documentation our parents sign.
- School social media content must not disclose unnecessary personal information about pupils, must avoid tagging pupils, and must be checked for images, names, school uniform details, location information and any information that could increase safeguarding risk.
- Any inappropriate comments or messages are to be deleted and reported by the assigned individual to Facebook, the Online safety coordinator and the safeguarding team in school.
- Any followers who do not meet the criteria for the page are blocked.

The internet in school

- Our school will maintain appropriate filtering and monitoring systems to help prevent access to harmful and inappropriate content while not unreasonably restricting teaching and learning. Filtering and monitoring roles and responsibilities are assigned to the DSL/safeguarding team, senior leaders, governors and IT support. The school currently uses an appropriate monitoring system which is reviewed regularly.
- Weekly reports are sent to the DSL and DDSL and urgent alerts are followed up promptly.
- Filtering and monitoring provision will be reviewed at least annually, and sooner if there is a safeguarding incident, system change, new technology, new device rollout, new AI tool or a concern that filtering or monitoring is not effective.
- The internet in school is filtered by Entrust Education and provided through Entrust Education. The school will liaise with Entrust/IT support to ensure filtering categories and monitoring alerts reflect current risks, including harmful content, radicalisation, self-harm, pornography, violence, gambling, scams, malware, AI chatbots and tools capable of generating or manipulating inappropriate images.

- Endpoint protection, security updates and patching will be maintained on school devices. The school will also work with IT support to follow DfE cyber security standards, including secure configuration, backups, access control, prompt software updates and incident response planning.
- If pupils come across any inappropriate content or have any issues they should click the report button (CEOP), minimise the screen and tell an adult immediately. The website should be minimised instead of closed so that the member of staff can obtain the URL. The incident should then be reported to the online safety coordinator and a safeguarding officer who will then investigate and inform Entrust Broadband of the URL requiring blocking if investigations dictate that this is needed.
- Pupils are only allowed to use the internet when an adult is present and all computing devices have internet history so that we can track internet usage.
- You Tube is only allowed to be used by members of staff for teaching purposes and must never be accessed by children without close adult supervision.
- Children sign and agree to an acceptable use policy which is approved by their parent/ carer.
- Children can also use the Confide software linked to our safeguarding practice. This will email selected staff and always the Designated Safeguard Lead.
- Mobile phones and personally owned smart devices are not used by pupils during the school day unless specifically authorised for a planned educational or individual need. Further details can be found in the school's Mobile Phone and Smart Technology Policy.

Staff usage

- Staff may access You Tube but may only display a video which has been risk assessed prior to showing the pupils.
- Staff may upload to our school Youtube channel if the video does not contain children and is uploaded as a child safe post.
- Staff must not access social media sites on the school premises (except Facebook for the purpose of posting on the school page) and should maintain the professional conduct while using the internet in line with the professional conduct strand of the teaching standards. Please see the school policy on social media usage for more information.
- Staff must use email respectfully and responsibly and understand that the technician has access to any email account should the need arise for an investigation into inappropriate use.
- Staff should model outstanding online safety awareness to pupils in their own use of the internet in lessons and should ensure that relevant online safety teaching points are embedded in their teaching.
- Staff must report suspected cyber incidents, phishing emails, account compromise, malware, ransomware or data breaches immediately to the headteacher/DSL, DPO where relevant and IT support, following school data protection and incident response procedures.
- Staff must not access their personal email account (except for the learning platform) using the school internet system unless it can be proven that it is for the retrieval of an educational resource.
- *Staff emails must not be opened in front of any child in school- with particular reference to the display on the IWB. Notifications should also be disabled.*
- Staff must not enter pupil personal data, safeguarding information, assessment data or confidential school information into unapproved AI tools, websites or apps. Any use of AI must be authorised, age-appropriate, transparent, checked for accuracy and compliant with data protection and safeguarding expectations.

Introducing new technology in school

- All technology, software, apps, online platforms and AI tools are risk assessed in terms of online safety, safeguarding, data protection, accessibility, age-appropriateness, educational value and potential impact upon learning before use with pupils.
- If a device, software platform or AI tool is deemed to be a valuable teaching and learning resource, privacy settings, data protection checks, filtering, monitoring, access controls, age restrictions and staff guidance must be in place before pupil use.

- New devices, platforms or AI tools will be accompanied by staff guidance/training where required, and children will receive relevant online safety teaching before independent or supervised use.
- The introduction of new devices will be reviewed by the online safety coordinator, Computing leader, Head teacher, Safe guarding officer, ICT technician and governors.

Staff training

At Amington Heath, we recognise that our staff need the most up to date information to be able to deliver an effective online safety curriculum. We also acknowledge our role in ensuring we provide training which helps to keep our staff safe online and help them to meet the professional conduct strand of the teaching standards.

- Staff will receive annual training in online safety/online safety, filtering and monitoring, cyber security, social media use, data protection, AI risks, image-based abuse, harmful online content, online sexual harassment, youth-produced sexual imagery and reporting routes. New staff will receive this information as part of induction.
- Staff will complete an acceptable usage policy document.
- Additional support will be provided where required and such training will always be provided to new members of staff before delivering the online safety curriculum.

Governors training

While governors play an essential role in the development and reviewing of the online safety policy, it is crucial that we provide appropriate training so that they are fully aware of their responsibility in ensuring whole school online safety. It is also essential that we provide governors with an understanding of how they themselves can remain safe online.

- Governors to receive an online safety update from the online safety coordinator and/or an external provider annually.
- Online safety is annually on the governing body agenda.
- A governor is designated for Online safety and work alongside other professionals to monitor and assess its effectiveness and impact.
- Governors will ensure that filtering and monitoring standards are reviewed at least annually, including checks that roles are assigned, systems are effective, reports are acted upon and staff understand how to report concerns.
- Governors receive cyber security, filtering and monitoring and online safety updates in line with KCSIE, DfE digital and technology standards and school safeguarding requirements.

Parental involvement

With technological advancements and the now ease of access to the internet it is more important than ever to ensure we engage with parents surrounding online safety. As a school we have two responsibilities: ensuring parents can support their child with online safety and the parents own online safety.

- We provide updates of online safety for both parents and their children through stands at the termly parents evening.
- We engage parents through coffee mornings to discuss current issues and concerns.
- Parents are invited to whole school assemblies with an online safety focus.
- Parents are also invited to engage in inspire workshops and meetings with external agencies.
- Parents are required to sign an acceptable use policy which details the schools requirements for their children.
- Parents and carers will be signposted to guidance on privacy settings, reporting harmful content, managing screen time, age ratings, online gaming, social media, AI-generated content, deepfakes, scams and image-sharing risks.

Reaching out to the wider community

- The online safety lead aims to engage with members of external agencies who can work with our families to develop their online safety.
- By working as a cluster of schools we aim to share best practice between schools and reach more members of the community.

Online Safety Oversight

Online safety forms part of the school's wider safeguarding arrangements.

Strategic oversight is provided by the Headteacher, Designated Safeguarding Lead, Online Safety Coordinator and Governing Board.

Online safety, filtering and monitoring, cyber security, staff training, emerging technologies and AI related risks are reviewed regularly through leadership meetings and governor monitoring activities. Feedback from pupils, parents, staff and safeguarding processes is considered when evaluating the effectiveness of online safety provision.

The Governing Board receives regular updates regarding online safety and fulfils its statutory responsibilities through existing governance arrangements rather than a separate committee structure.

Risk Assessment

Amington Heath will regularly audit ICT/computing provision to ensure it is safe for children's use. The school will complete an annual online safety risk assessment, supported by filtering and monitoring review information, safeguarding records, pupil voice, staff feedback and current national guidance. While precautions are in place and staff remain vigilant, it is possible for pupils to come across inappropriate material. In the unlikely event that this occurs, pupils and staff will follow the reporting guidelines in this policy. The school and Staffordshire LA do not accept liability for material accessed despite reasonable safeguards; this is detailed within the parental acceptable use policy.

Report an issue

Children should...

1. Use the report button
2. Minimise the screen
3. Tell an adult immediately
4. **Do not share, forward, screenshot or save harmful material unless specifically directed by a DSL for safeguarding evidence handling.**

Staff should...

1. Retrieve as much information as possible including the URL
2. Staff should reassure the pupil
3. Report the incident as soon as possible to a safeguarding officer and the online safety coordinator.
4. If an incident involves nude/semi-nude images, AI-generated sexual content, online sexual harassment, suspected grooming, radicalisation, self-harm content, cyberbullying or criminal behaviour, staff must follow safeguarding procedures immediately and seek DSL advice before viewing, copying or deleting any material.

Complaints

Any online safety/online safety complaint must be dealt with by a member of the senior leadership team and, if required, the headteacher. All safeguarding and child protection concerns must be managed in line with the school safeguarding and child protection policy, Keeping Children Safe in Education, Working Together to Safeguard Children, the Data Protection Act 2018, UK GDPR and relevant school behaviour, anti-bullying, mobile phone, acceptable use and social media policies.

General advice to teachers

- Ensure that children understand the importance of online safety.
- Refer to online safety in terms of content, contact, conduct and commerce.
- Teaching should be appropriate to the age and ability of the child, and may vary across year groups and key stages but should be linked to the Internet Safety Progression Ladder.
- Embed online safety across the curriculum and do not limit it to the Computing lesson.

- Create a safe and welcoming ethos where pupils feel able to report issue.
- Always report issues following the guidance in this policy as quickly as possible after the incident.
- Staff should pay particular reference to child-on-child abuse, online sexual harassment, cyberbullying, youth-produced sexual imagery, AI-generated or manipulated sexual images, deepfakes, harmful online challenges, radicalisation, self-harm content and online exploitation as set out in KCSIE 2025 and subsequent statutory guidance. These themes are embedded through Computing, PSHE/RSHE and wider safeguarding practice.

Monitoring and review

We are aware of the need to monitor and update the school's online safety policy on a regular basis, so that we can take account improvements made in our practice. We will therefore review this policy yearly, or earlier if necessary. Ongoing informal reviews and discussions will take place throughout the year through the online safety lead.

Key 2026 review sources considered: KCSIE 2025; draft KCSIE 2026 consultation; Working Together to Safeguard Children 2026; DfE Teaching Online Safety in Schools; DfE filtering and monitoring core standards; DfE cyber security standards; DfE generative AI in education and AI product safety standards; DfE mobile phones in schools guidance.

Appendix 1

Internet Safety Progression Ladder

Nursery	- Children know to tell an adult if they see something that upsets them. - Children know the need to close pop ups on the computer and apps. - Children know that they should only access the internet with adult permission and presence. - Children know that trusted adults help them when something online feels wrong.
Reception	- Children know they should only take photos of people with their permission. - Children know what to do if they feel sad or uncomfortable when using a computer or tablet. - Children know that they shouldn't tell a stranger their name, school or age. - Children know how to close pop ups on the computer and apps. - Children should pick technology appropriate to the task. - Children know they should ask before using a new app, website or device.
Year 1	- Children know to say 'kind words' to others through computing devices. - Children know that they shouldn't talk to strangers on the internet. - Children can define the term personal information and know that they should keep it private. - Children know how to use the report button online. - Children know who to tell about an online incident at school and home. - Children know that not everything online is true and they should ask an adult if they are unsure.
Year 2	- Children are respectful online. - Children know how to select appropriate information in a search engine. - Children know what content is inappropriate for their age. - Children can define personal information and know how they can keep it private. - Understand the term contact and consider what contact is appropriate and inappropriate. - Children can identify simple examples of online scams, adverts and requests for personal information.
Year 3	- Children use email safely and respectfully and know that they shouldn't disclose personal information through email. - Recognize unacceptable behavior online.

	- Children know how to report an issue online in school and at home. - Children can apply their understanding to tablets, desk tops and laptops. - Children identify their responsibility to report issue. - Children understand that images and videos can be edited and may not always show the truth.
Year 4	- Children are aware of 'junk' mail and potential risks within them. - Children recognize acceptable and unacceptable behavior online. - Children know how to protect information about themselves online. - Children can apply their understanding to tablets, desk tops, laptops, game consoles and mobile phones. - Children identify the responsibility for their comments and interactions online. - Children understand that AI tools can make mistakes and can create realistic but false images, voices or information.
Year 5	- Children are aware of pops up and how to control the pop up blocker. - Children know unacceptable behavior online can affect others. - Children know how to get things removed from social media websites. - Children can apply their understanding to any device. - Children identify their responsibility for the protection of their personal information. - Children understand misinformation, persuasive design, online pressure, in-app purchases and the importance of reporting harmful contact or content. - Children understand that sharing images without consent, including edited or AI-generated images, can cause serious harm.
Year 6	- Children understand how and why the school system is filtered, how they can filter at home and issues to be aware of when using unfiltered internet. - Children know how unacceptable behavior can affect their futures. - Children understand the term digital identity. - Children know how to have information about them removed from websites and google. - Children can identify ways in which they need to be responsible internet users. - Protecting against Peer on peer abuse - Safeguarding against Youth sharing of sexualized images

	- Children understand digital footprints, privacy settings, reporting routes, online reputation, deepfakes, scams, phishing and the risks of sharing personal or sexualised images. - Children understand that AI-generated content must be checked carefully and must not be used to impersonate, bully, embarrass or harm others.
--	---