E SAFETY, AI and ACCEPTABLE USE POLICY

Date policy reviewed	Autumn 2026
Date for next review	Autumn 2027
Committee responsible	FGB

HANSLOPE PRIMARY SCHOOL

1. EFFECTIVE PRACTICE IN E-SAFETY

At Hanslope Primary School, we know that E-Safety depends on effective practice in each of the following areas:

- Education for the responsible use of ICT by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from Integrated Tech
- A school network that complies with the National Education Network standards and specifications.
- Writing and reviewing the e-safety policy
- The child protection policy reflects that children with special educational needs or disabilities (SEND), or certain medical or physical health conditions can face additional barriers, including cognitive understanding (being unable to understand the difference between fact and fiction in online content and then repeating the content/behaviours in schools or colleges, or the consequences of doing so).

We are deeply committed to Safeguarding & Child Protection. This Policy therefore needs to be read in conjunction with the following:

- Child protection Policy
- Acceptable Use Protocol (see below)
- Behaviour/Anti-Bullying Policy
- Health and Safety Policy
- Policy on Social Networking Sites & Personal Internet Presence for School Staff

Our e-Safety Policy has been written by the school.

2. TEACHING AND LEARNING

2.2.1 Why the Internet and digital communications are important

We appreciate that the Internet is an essential element in 21st century life for education, business and social interaction. Hanslope Primary School has 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.

2.2.2 Internet use will enhance learning

- Hanslope Primary School's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. E safety is a core part of the computing curriculum and teachers must ensure that children leave the school able to: "use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet" NC 2014
- 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 shown how to "use technology purposefully to create, organise, store, manipulate and retrieve digital content." NC 2014

2.2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content

2.3 MANAGING INTERNET ACCESS

2.3.1 Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with ICT consultants and broadband suppliers

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail, to both pupils and staff, should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Staff email addresses are only for school use.

2.3.3 Published content and the school web site

- Staff school emails will be published and should be checked on a regular basis.
- Pupil personal contact information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil's images and work

- The use of individual photographs will be discouraged and the school will not publish the names of children alongside any such photographs.
- Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs. Names of school council members may be published on the website.
- Permission from parents or carers will be obtained before photographs of pupils are published (this includes in newspapers, on the school websites and social media).
- Pupils work maybe published, parental/carers permission will be sought where appropriate.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.3.5 Social networking and personal publishing

- The school will control access to social networking sites, and educating pupils in their safe use will form part of E-safety teacher.
- Message boards/ forums 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, their friends or their location.
- Pupils will not use social networking sites in school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.3.6 Managing filtering

- The school will work with Integrated Tech to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator (Mrs Lovegood).
- Regular checks by our IT support company are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.
- When not in use webcams on teacher laptops should be disabled to prevent malicious use.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with data enabled can bypass school filtering systems and present a new route to undesirable material and communications.
- Pupils mobile phones will not be used at school and must be given to the class teacher who will store it in their cupboards until the end of the day.
- Games machines including the Sony Playstation, Microsoft Xbox and others must not be used to access the Internet at school, and must be used in accordance with the AUP.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

2.4 POLICY DECISIONS

2.4.1 Authorising Internet access

- All staff and Governors must read and sign the "Staff Code of Conduct for ICT" before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access

to school ICT systems.
- At Key Stage 1, access to the Internet will be following adult demonstrations with directly supervised access to specific, approved on-line materials.
- At Key Stage 2 children will be directed to specific sites, which have been checked by the teacher prior to use.
- Any person not directly employed by the school will not have access to the Internet.

2.4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see child protection policy).
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Misuse and on-line bullying

Children and young people are keen adopters of new technologies, but this can also leave them open to the threat of increased bullying - known as online bullying, e-bullying or cyber-bullying. This form of bullying can be defined as follows:

“The use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others”

Bullying can take the form of:

- Text messaging
- Email
- Chat and Social Networking – this should not be an issue for pupils at our school due to age, however we are aware that this requirement can be inadvertently overlooked by parents, if they fail to read the terms and conditions of use, or their child as signed up without seeking their permission
- Instant Messaging

All reported incidents of IT misuse and cyber-bullying will be dealt with in accordance with our Behaviour/Anti-Bullying Policy. We do not see cyber-bullying as any less serious as non-electronic bullying and our standard policies, strategies and sanctions apply.

2.4.4 Community use of the Internet

- Currently the school does not provide community access to the internet.
- The school will promote community awareness of e-safety through the school website or through the usual methods of parental communication, where appropriate.

2.5 COMMUNICATIONS POLICY

2.5.1 Introducing the e-safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of lessons in e-Safety will be followed, based on the materials from 'Project Evolve' (see 'Hanslope School E-safety progression' document.
- E-Safety training will be embedded within the ICT scheme of work.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

2.5.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

3 – AI Policy

3.1 Statement of intent

At Hanslope Primary School, we recognise that the use of artificial intelligence (AI) can help to positively affect teacher workload, develop pupils' intellectual capabilities and prepare them for how emerging technologies will change workplaces. While there are many benefits to the use of AI tools, the content they produce may not always be accurate, safe or appropriate, and could lead to malpractice.

Through the measures outlined in this policy, the school aims to ensure that AI is used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace.

For the purposes of this policy, the following terms are defined as:

- **AI** – The theory and development of computer systems able to perform tasks normally requiring human intelligence, e.g. visual perception, speech recognition, decision-making.
- **Generative AI** – A category of AI algorithms that generate new outputs based on the data they have been trained on.
- **Misuse of AI** – Any use of AI which means that pupils have not independently demonstrated their own attainment.

3.2 Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- DfE (2026) 'Keeping children safe in education 2026'
- DfE (2023) 'Generative artificial intelligence in education'
- DfE (2023) 'Meeting digital and technology standards in schools and colleges'
- JCQ (2023) 'Artificial Intelligence (AI) Use in Assessments: Protecting the Integrity of Qualifications'
- JCQ (2023) 'Suspected Malpractice Policies and Procedures'

This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy

3.2.1 Roles and responsibilities

The headteacher will be responsible for:

- Ensuring that the use of AI tools in the school is integrated into relevant policies and procedures, the curriculum and staff training.
- Communicating with parents to ensure they are kept up-to-date with how AI tools are being used in the school, how this will impact pupils' education and how the school is ensuring the tools are being used safely and effectively.
- Working with the Computing Lead and school DSL to review and update this policy on an annual basis.
- Ensuring that AI practices are audited and evaluated on a regular basis.

Computing Lead will be responsible for:

- Providing technical support in the development and implementation of the school's AI practices, policies and procedures.
- Implementing appropriate security measures.
- Ensuring that staff receive regular, up-to-date training on how to use AI tools in school.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in school.
- Undertaking training so they understand the risks associated with using AI tools in school.
- Liaising with relevant members of staff on online safety matters.
- Maintaining records of reported online safety concerns relating to the use of AI tools, as well as the actions taken in response to concerns.

All staff members will be responsible for:

- Adhering to the Acceptable Use Agreement as part of this E-Safety Policy and other relevant policies.
- Taking responsibility for the security of the AI tools and data they use or have access to.
- Modelling good online behaviours when using AI tools.

- Maintaining a professional level of conduct in their use of AI tools.
- Having an awareness of the risks that using AI tools in school poses.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring that the safe and effective use of AI tools is embedded in their teaching of the curriculum.
- Familiarising themselves with any AI tools used by the school and the risks they pose.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from the relevant school staff if they are concerned about an experience that they or a peer has experienced while using AI tools.
- Reporting concerns in line with the school's reporting procedure.
- Familiarising themselves with any AI tools used by the school and the risks they pose.

3.3 Data protection and cyber-security

The school is aware of the data privacy and cyber-security implications that come with using generative AI tools. The school will follow the procedures in these policies to continue to protect pupils from harmful online content that could be produced by AI tools.
The school will not enter data that is classed as personal and sensitive into public AI tools under any circumstances. Any data entered will not be identifiable and will be considered released to the internet.
All staff will apply their best judgement and common sense to manage cyber-security risks effectively and ensure that the DfE's cyber standards are followed at all times.
The school will:

- Protect personal and special category data in accordance with data protection legislation.
- Not allow or cause intellectual property, including pupils' work, to be used to train generative AI models, without appropriate consent or exemption to copyright.
- Review and strengthen cyber security by referring to the DfE's cyber standards.
- Be mindful that generative AI could increase the sophistication and credibility of cyber attacks.
- Ensure that pupils are not accessing or creating harmful or inappropriate content online, including through AI tools.
- Refer to the DfE's Filtering and monitoring standards for schools and colleges to ensure that the appropriate systems are in place.
- Be mindful of the data privacy implications when using AI tools and will take steps to ensure that personal and special category data is protected in accordance with data protection legislation.

If it is necessary to use personal and special category data in AI tools, the school will ensure that the tools comply with data protection legislation and existing privacy policies to protect the data.
The school will be open and transparent whilst ensuring that data subjects understand their personal or special category data is being processed using AI tools.

3.4 Using AI tools

The school will ensure that AI tools are used appropriately to achieve the following aims:

- To reduce workload
- To free up teachers' time

- To assist with the production of high-quality and compliant administrative plans, policies and documents
- To support the teaching of a knowledge-rich computing curriculum
- To teach pupils:
    - How to use emerging technologies safely and appropriately.
    - About the limitations, reliability and potential bias of AI tools.
    - How information on the internet is organised and ranked.
    - How online safety practices can protect against harmful and misleading content.
    - To identify and use appropriate resources to support their education, including age-appropriate resources and preventing over-reliance on a limited number of tools or resources.

Whilst recognising that AI tools can be used appropriately and with benefit to teaching and learning, the school will keep in mind that the content produced by AI tools can be:

- Inaccurate.
- Inappropriate.
- Biased.
- Taken out of context and without permission.
- Out of date or unreliable.

Where AI tools are used to produce administrative plans, policies and documents, all staff members will understand that the quality and content of the final document remains the professional responsibility of the staff member who produced it. Staff members using AI tools to create documents will not assume that AI output will be comparable with a human-designed document that has been developed in the specific context of the school.
Pupils will be made aware of the importance of referencing AI tools correctly when using AI tools to produce work, especially if the work is for an assessment, in order to allow teachers and assessors to review how AI has been used and whether it was appropriate. Pupils' references to AI sources will show the name of the AI source and the date that the content was generated.
Pupils will retain a copy of the questions and AI generated content for reference and authentication purposes in a non-editable format, e.g. a screenshot. Pupils will also provide a brief explanation of how AI tools have been used.
When using AI tools, staff and pupils will ensure that any content produced is scrutinised and cross-checked for its appropriateness and accuracy.
Staff members will be aware that AI tools return results based on the dataset it has been trained on – it may not have been trained on the national curriculum, and may not provide results that are comparable with a human-designed resource developed in the context of the national curriculum. Staff members will be mindful of this in their teaching and marking of pupils' work.
Pupils and staff members will be reminded that using AI tools cannot replace the judgement and deep subject knowledge of a human expert. Staff members will stress the importance of pupils acquiring their own knowledge, expertise and intellectual capability rather than relying on AI tools in their work.
The school will not allow or cause pupils' original work to be used to train AI tools.

3.5 Misusing AI tools

Preventing misuse
The school acknowledges that misuse of AI tools can happen both accidentally and intentionally, and that education and awareness is key to preventing misuse. The school will consider taking the following actions to prevent the misuse of AI tools:

- Restricting access to online AI tools on school devices and networks, especially on devices used for exams and assessments

- Setting reasonable deadlines for submission of work and providing pupils with regular reminders
- Allocating time for sufficient portions of pupils' work to be completed in class under direct supervision, where appropriate
- Examining intermediate stages in the production of pupils' work to ensure that work is being completed in a planned and timely manner, and that work submitted represents a natural continuation of earlier stages
- Introducing classroom activities that use the level of knowledge and understanding achieved during lessons to ensure the teacher is confident that pupils understand the material
- Engaging pupils in verbal discussions about their work to ascertain that they understand it and that it reflects their own independent work
- Refusing to accept work that is suspected to have been generated through misuse of AI tools without further investigation
- Issuing tasks which are, wherever possible, topical, current and specific, and require the creation of content which is less likely to be accessible to AI models
- Investing in educating and training staff, pupils and parents on the use of AI tools and raising awareness of the risks and issues that come with its use

3.6 Identifying misuse

Staff members will continue to use the skills and observation techniques already in use to assure themselves that pupils' work is authentically their own when attempting to identify a misuse of AI tools.

When reviewing pupils' work to ensure its authenticity, staff members will compare it against other work created by the pupil. Where the work is made up by writing, the staff members will make note of:

- Spelling and punctuation.
- Grammatical usage.
- Writing style and tone.
- Vocabulary.
- Complexity and coherency.
- General understanding and working level.
- The mode of production, i.e. whether the work was handwritten or word-processed.

Staff members will be aware of and look out for potential indicators of AI use, which include:

- A default use of American spelling, currency, terms and other localisations.
- A default use of language or vocabulary which might not be appropriate to the working or qualification level.
- A lack of direct quotations and/or use of references where these are required or expected.
- Inclusion of references which cannot be found or verified.
- A lack of reference to events occurring after a certain date, reflecting when an AI tool's data source was compiled.
- Instances of incorrect or inconsistent use of first-person and third-person perspective where AI generated text has been left unaltered.
- A variation in the style of language evidenced in a piece of work, if a pupil has taken specific portions of text from an AI tool and then amended it.
- A lack of graphs, data tables or visual aids where these would normally be expected.
- A lack of specific, local or topical knowledge.
- Content being more generic in nature.

- The inadvertent inclusion of warnings or provisos produced by AI tools to highlight the limits of its ability or the hypothetical nature of its output.
- The submission of pupil work in a typed format, where this is not usual, expected or required.
- The unusual use of several concluding statements throughout the text, or several repetitions of an overarching essay structure within a single lengthy essay.
- The inclusion of confidently incorrect statements within otherwise cohesive content.

Staff members will remain aware that AI tools can be instructed to employ different languages and levels of proficiency when generating content, and some are able to produce quotations and references.

3.7 Exams and assessments

The school will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI tools regarding exams and assessments.
Pupils will be made aware of the appropriate and inappropriate uses of AI tools, and the consequences of its misuse. Pupils will be made aware that it is not acceptable to submit work that has been produced with an AI tool, and of the school's approach to plagiarism and malpractice. Pupils will also be made aware of the risks of using AI tools to complete exams and assessments, which include:

- Submitting work that is incorrect or biased.
- Submitting work that provides dangerous and/or harmful answers.
- Submitting work that contains fake references.

Staff members will discuss the use of AI tools and agree a joint approach to managing pupils' use of AI tools in the school.
Pupils will only be permitted to use AI tools to assist with assessments where the conditions of the assessment permit the use of the internet, and where the pupil is able to demonstrate that the final submission is the product of their own independent work and thinking.
Pupils in KS2 will be required to sign a declaration to confirm that they understand what AI misuse is, and that it unacceptable. Pupils will be made aware of the consequences of submitting a false declaration, and any AI misuse'.

Copying or paraphrasing sections, or whole responses, of AI generated content

- Using AI to complete parts of the assessment so that the work does not reflect the pupil's own work, analysis, evaluation or calculations
- Failing to acknowledge the use of AI tools when they have been used as a source of information
- Incomplete or poor acknowledgement of AI tools
- Submitting work with intentionally incomplete or misleading references and/or bibliographies

3.8 Safeguarding

The school acknowledges that generative AI tools can be used to produce content that is dangerous, harmful, and inappropriate. The school will follow the procedures set out in the Child Protection and Safeguarding Policy and this E-Safety Policy to ensure that pupils are not able to access or be exposed to harmful content.
Pupils will be taught about the risks of using AI tools and how to use them safely. Pupils will be made aware of how to report any concerns or incidents involving generative AI, and who to talk to about any issues regarding the use of AI tools.

The school will ensure that parents are aware of who to speak to about any concerns or issues regarding the use of AI.
The school will ensure that the appropriate filtering and monitoring systems are in place to protect pupils online, following the DfE's filtering and monitoring standards.
All staff members will receive training on the safe use of AI as part of their online safety training, which is regularly updated.

3.9 Teaching pupils about the safe use of AI

Teaching about the safe and appropriate use of AI will ensure that pupils benefit from a knowledge-rich curriculum which enables them to become well-informed users of technology and understand its impact on society. Pupils will gain strong foundational knowledge which ensures they are developing the right skills to make the best use of AI tools.
The school will:

- Prepare pupils for changing workplaces.
- Teach pupils how to use emerging technologies, including AI tools, safely and appropriately.
- Raise awareness of the limitations, reliability and potential bias of AI tools.
- Help pupils to understand how information on the internet is organised and ranked.
- Include online safety teaching in the curriculum and how to protect against harmful or misleading content.
- Raise awareness and understanding of protecting intellectual property rights.
- Encourage the safe and responsible use of digital content.
- Teach about the impact of technology, including disruptive and enabling technologies.
- Include teaching about how computers work, connect with each other, follow rules and process data in the curriculum.

Pupils will be supported to identify and use appropriate resources to support their ongoing education through the use of age-appropriate resources, which may include AI tools, whilst preventing over-reliance on a limited number of tools or resources.

3.10 Monitoring and review

Computing Lead and headteacher will review this policy in full on an annual basis, and following any incidents that occur due to the use of AI tools, e.g. data protection or cyber-security.
Any changes made to this policy are communicated to all members of the school community.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Learning Zone
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. 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.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	SuperClubs Plus School Net Global
Publishing pupils' work on school and other websites.	Pupils" full names and other personal information should be omitted. Pupils" work should only be published on „moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History Kent Grid for Learning Cluster Microsites National Education Network Gallery
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. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Audio and video conferencing to gather information and share pupils" work.	Pupils should be supervised.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers and parents

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World
www.dfes.gov.uk/byronreview/
Project Evolve
https://projectevolve.co.uk/

Appendix 3: Useful resources for parents

Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Internet Safety Zone
www.internetsafetyzone.com