



Huntington Community Primary School

Online Safety Policy

2026

Headteacher	David Erne	Signed / Date:
Chair of Governors	Amanda Robinson	Signed / Date:
Date approved by governing board		
Next full review due	Autumn 2027 (moving to annual review — see section 24)	

Document control

Version	Date	Summary of changes	Author
1	Nov 2023	Original policy adopted.	—
2	Aug 2026	Reviewed and updated to reflect: Keeping Children Safe in Education 2026 (in force 1 September 2026), including the new ‘nudes’ terminology and its extension to AI-generated/deepfake imagery; the updated DfE Filtering and Monitoring Standards (June 2026), including AI-generated content, BYOD and mandatory blocking of illegal content; the DfE Mobile Phones in Schools guidance (Jan 2026 update); the updated DfE Generative AI in Education guidance (Aug 2025); the updated Sharing Nudes and Semi-Nudes advice (Mar 2024); the Online Safety Act 2023 as context; and the Data (Use and Access) Act 2025. Review cycle moved from three-yearly to annual. See individual sections for detail.	D Erne, Headteacher

Contents

Statement of intent

1. Legal framework

2. Roles and responsibilities

3. Managing online safety

4. Cyberbullying

5. Child-on-child sexual abuse and harassment

6. Grooming and exploitation

7. Mental health

8. Online hoaxes and harmful online challenges

9. Cyber-crime

10. Online safety training for staff

11. Online safety and the curriculum

12. Use of technology in the classroom

13. Use of smart technology and mobile phones

14. Educating parents

15. Internet access

16. Filtering and monitoring online activity

17. Network security

18. Emails

19. Generative artificial intelligence (AI)

20. Social networking

21. The school website

22. Use of devices

23. Remote learning

24. Monitoring and review

Appendix A: E-Safety Agreement

Appendix B: E-Safety Rules – KS1 and KS2

Appendix C: Staff (and Volunteer) Acceptable Use Policy Agreement

Appendix D: Community Users Acceptable Use Policy Agreement

Appendix E: Record of Reviewing Devices / Internet Sites

Appendix F: School Reporting Log

Appendix G: School Training Needs Audit

Statement of intent

Huntington Community Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- Online Safety Act 2023 — this places statutory duties on online platforms and search services (not on schools directly) to protect children from illegal and harmful content; it forms the backdrop against which this policy's curriculum and reporting provisions operate
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- DfE (2026) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping Children Safe in Education' (statutory guidance, in force from 1 September 2026)
- DfE (2023) 'Teaching online safety in schools'
- DfE (2023) 'Searching, screening and confiscation'
- DfE (2026) 'Mobile phones in schools' guidance
- DfE (2025) 'Generative artificial intelligence (AI) in education'
- DfE (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Staff Disciplinary Policy and Procedure
- Data Protection Policy
- Use of Mobile Phones and Digital Photography Policy
- Remote Education Policy

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant law and statutory guidance, including Keeping Children Safe in Education 2026.
- Ensuring the DSL's remit explicitly covers online safety.
- Formally reviewing and ratifying this policy on an annual basis, or sooner following a significant online safety incident or a major change in statutory guidance (see section 24).
- 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 and at regular intervals, and that this training addresses filtering and monitoring roles and responsibilities.
- Ensuring that there are appropriate filtering and monitoring systems in place, and designating specific governor and senior leadership oversight of this area in line with the DfE's Filtering and Monitoring Standards.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher will be responsible for:

- 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 DSL and the deputy DSL 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, including in relation to generative AI and filtering and monitoring.
- Ensuring online safety practices are audited and evaluated.
- 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 and ICT technicians to conduct the annual review of this policy.

The DSL (currently the headteacher) will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCo and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school, including how they address AI-generated and dynamic content, and reviewing this understanding annually.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems.
- Ensuring that all staff read Part One of Keeping Children Safe in Education 2026 in full — rather than a summarised annex — as part of induction and annual updates, given the online safety content integrated throughout it.
- 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 at least annually.
- Working with the headteacher (if not the DSL) and ICT technicians to conduct the annual review of this policy.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate, including their ability to address AI-generated and dynamic content.
- Working with the DSL and headteacher to conduct the annual review of this policy.

All staff members will be responsible for:

- 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, including how AI-generated content (e.g. deepfakes) can be used to cause harm.
- 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.

Pupils will be responsible for:

- Adhering to the E-Safety 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 in line with the procedures within this policy.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from the deputy DSL and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training, utilising resources from SWGfL and elsewhere.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum (and specifically within the Project Evolve scheme adopted within the Computing curriculum).
- Assemblies are conducted termly on the topic of remaining safe online, including the annual Safer Internet Day assembly in February.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may still be shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully — the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils (e.g. calling the police) where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

All online safety incidents and the school's response are recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse
- Discriminatory bullying online, i.e. homophobia, racism, misogyny/misandry

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur, in line with the Anti-Bullying Policy.

5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of nude and semi-nude images and videos (sometimes referred to as 'sexting'), including images that have been digitally altered or wholly generated using artificial intelligence ('deepfakes' or 'deep nudes')
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children (i.e. individuals under the age of 18) is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves, and even where the imagery has been digitally altered or generated using AI so that it depicts a real child.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-Child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-Child Abuse Policy and the Safeguarding and Child Protection Policy.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been

manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils in relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, via Prevent Duty training. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty guidance.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an “online hoax” is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, “harmful online challenges” refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online — the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source (e.g. the UK Safer Internet Centre) when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Safeguarding and Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** — these crimes can be carried out offline; however, they are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** — these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. Training will also cover how generative AI and other emerging technologies can be used to create or facilitate harm, e.g. AI-generated 'deepfake' or 'deep nude' imagery. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and health education
- PSHE
- Computing (via Project Evolve resources especially)

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. A comprehensive list of such risks can be found within Teaching Online Safety in Schools (DfE, 2023).

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff (e.g. the SENDCo and designated teacher for LAC) will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms (e.g. pupils with SEND and LAC) receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding and Child Protection Policy.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Desktop computers
- Laptops and Chromebooks
- Tablets (Learnpads)
- Internet (e.g. Google Classroom)
- Email
- Digital cameras and microphones

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time — this supervision is suitable to their age and ability.

13. Use of smart technology and mobile phones

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's E-Safety Agreement for Pupils.

In line with the DfE's Mobile Phones in Schools guidance, Huntington Community Primary School operates as a phone-free environment for pupils during the school day. Pupils are not permitted access to personal devices within school; Y5/6 children may carry a mobile phone to enhance their safety during the journey to/from school, but this is handed in and retained by the class teacher in a secure area for the duration of the school day. Reasonable adjustments to this arrangement will be considered on an individual basis for pupils who need a personal device for medical or SEND-related reasons, agreed in advance with the headteacher.

Staff will use all smart technology and personal technology in line with the school's Acceptable Use Policy.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually, including AI-generated or 'deepfake' images.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology anywhere on the school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement on entry and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.

- Sharing of nude or semi-nude images of pupils (including AI-generated or 'deepfake' images).
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parent workshops
- Newsletters
- Online support (e.g. school website's Online Safety page)

15. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the E-Safety Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filtering and monitoring systems in place and that it is meeting the DfE's Filtering and monitoring standards for schools and colleges (2026). The governing board will designate specific senior leadership and governor oversight of filtering and monitoring, and will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regard to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. In line with the updated DfE standards, the school will consider whether its filtering and monitoring solution can identify and respond to real-time, dynamic and AI-generated content, and this will be a specific factor in the annual review described below. ICT technicians will undertake termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Websites and content known to be illegal, e.g. child sexual abuse material and terrorist content, will always be blocked, and this cannot be switched off or overridden at school level.

Where the school operates a bring your own device (BYOD) scheme, personal devices connecting to the school's network will be subject to the same filtering standards as school-owned devices; unmanaged personal devices will connect via a separate network, and the school will confirm with its filtering provider that all internet feeds, including any portable wifi devices, are covered.

The effectiveness of the school's filtering and monitoring provision will be formally reviewed at least once every academic year, and additionally whenever a safeguarding risk emerges, technology changes, or a new tool is introduced. This review will consider the risk profile of the school's pupils, including those who may be more vulnerable, and will be reported to the governing board.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to ICT technicians immediately, who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Staff Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Safeguarding and Child Protection Policy.

17. Network security

Technical security features, such as anti-virus software, will be kept up to date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls regularly to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 2 and above will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Staff passwords will expire after 90 days, after which users will be required to change them.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

18. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff will be given approved school email accounts and will only be able to use these accounts at school or when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails — staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Any cyber-attacks initiated through emails will be managed in line with the school's business continuity and disaster recovery arrangements.

19. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies (e.g. generative AI) and how to use them safely and appropriately, with consideration given to pupils' age, in line with the DfE's Generative artificial intelligence (AI) in education guidance (2025).

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI, including AI-generated nude, semi-nude or otherwise sexualised imagery of real or apparent children ('deepfakes' or 'deep nudes').

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI, and will treat the creation or sharing of AI-generated indecent imagery of a child as seriously as if the imagery were real, in line with Keeping Children Safe in Education 2026.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

Before introducing any new generative AI tool for use by staff or pupils, the school will assess the associated risks against the DfE's product safety expectations for AI in education, and will make use of any further guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social networking

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

21. The school website

The headteacher will be responsible for the overall content of the school website — they will ensure the content is appropriate, accurate, up to date and meets government requirements.

22. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Acceptable Use Agreements.

23. Remote learning

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

24. Monitoring and review

The school recognises that the online world is constantly changing and that DfE statutory guidance in this area is now updated frequently — including Keeping Children Safe in Education, which is revised on an annual basis. The DSL, ICT technicians and the headteacher will therefore conduct an ongoing review of this policy's effectiveness throughout the year, and will check it specifically against the content of each September's updated Keeping Children Safe in Education.

The governing board, headteacher and DSL will formally review this policy in full on an annual basis, and following any online safety incident or major change to relevant legislation or statutory guidance.

The next scheduled review date for this policy is Autumn 2027, with the following full review due Autumn 2028, and so on annually thereafter unless brought forward.

Any changes made to this policy are communicated to all members of the school community.

APPENDICES

Appendix A: E-Safety Agreement

Appendix B: E-Safety Rules – KS1 and KS2

Appendix C: Staff (and Volunteer) Acceptable Use Policy Agreement

Appendix D: Community Users Acceptable Use Policy Agreement

Appendix E: Record of Reviewing Devices / Internet Sites

Appendix F: School Reporting Log

Appendix G: School Training Needs Audit

Appendix A: E-Safety Agreement

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the E-Safety Rules, which have been revised in consultation with classes Y1–Y6, have been understood and agreed.

Pupil name:	Class:
Pupil's agreement • I have read and I understand the school E-Safety Rules. • I will use school computers, our school website, internet access and other new technologies in a responsible way at all times. • I know that school computers, the school website and Google Classroom may be monitored.	
Signed:	Date:
Parent's consent for web publication of work I agree that my child's work may be electronically published (this does not refer to photographs including my child, for which separate permission must be sought). Parent's consent for internet access I have read and understood the school E-Safety Rules and give permission for my child to access the internet and Google Classroom. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, including use of a filtered internet service, but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the internet.	
Signed:	Date:
Please print name:	
Please complete, sign and return to the school office. Thank you.	

Appendix B: E-Safety Rules – KS1 and KS2



Learn to Live, Live to Learn

Think before you Click

E-Safety Rules for Key Stage 1

These rules help us to stay safe on the internet.

- We only use the internet when an adult is with us, and we always ask if we get lost.
- If we see something we don't like on the internet we tell an adult straight away.
- We only click on the buttons or links when we have been told what they do.
- We never let anyone know our passwords (except for our parents).
- We only write polite and friendly messages on the website and Google Classroom, to people that we know.
- We log out when we finish work.

E-Safety Rules for Key Stage 2

- We ask permission before using the internet.
- We immediately minimise any webpage we are uncomfortable with, and then tell an adult straight away.
- We only write polite and friendly messages on the website and Google Classroom, to people that we know.
- We tell an adult if someone sends us an unpleasant message.
- We never give out personal information or passwords, and we log out when we have finished working.
- We never upload photos of ourselves or other children.
- We never arrange to meet anyone we don't know.
- We never try to visit internet chat rooms.

Appendix C: Staff (and Volunteer) Acceptable Use Policy Agreement

School policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and support effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school technology systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers have good access to digital technology to enhance their work and pupils' learning opportunities, and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school technology systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the technology systems and other users. I recognise the value of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from its use. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school's digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, tablets, email, the school website and official school social media accounts) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school's digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may access it.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of to the appropriate person.

I will be professional in my communications and actions when using school digital technology systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will only use personal CDs/DVDs on school devices for curriculum purposes if the content is age appropriate (U certificate, in the case of BBFC classified video material).
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (e.g. mobile phone, USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use, including the school's phone-free arrangements for pupils. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's digital technology systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school's policies. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper-based documents containing personal data must be held in lockable storage.
- I understand that data protection law (the UK GDPR and the Data Protection Act 2018) requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, either by making an entry in the IT file or informing the headteacher directly.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school digital technology systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school's digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/volunteer name:	Signed:
	Date:

Appendix D: Community Users Acceptable Use Policy Agreement

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices.
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the headteacher.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programs of any type on a school device, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the headteacher.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.

I have read and understand the above and agree to use the school's digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:	Signed:	Date:
-------	---------	-------

Appendix E: Record of Reviewing Devices / Internet Sites

(for responding to incidents of misuse)

Class	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for websites)

Website(s) address / device — reason for concern

Conclusion and action proposed or taken

Appendix F: School Reporting Log

[illegible]

Appendix G: School Training Needs Audit

[illegible]