Hatch Warren Junior School

E-Safety Policy

2025-2026

Policy Author: Headteacher

Approved by: Full Governing Body

Approved on: 20th November 2025

Date of issue: November 2025

Review Date: November 2026

Contents:

Statement of intent

Hatch Warren Junior 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 and operates in conjunction with other relevant school policies.

2. Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSLs remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the school has effective levels of security protection procedures in place in order to safeguard their systems, staff and learners and that these procedures are reviewed periodically

The head teacher is 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 DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Keep parents up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing board to update and review this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- 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 SENCO, school business manager (SBM) and Computing lead
- 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Reviewing and acting upon online safety incidents and inappropriate internet use, both by pupils and staff and providing governors with an update termly
- Ensuring all members of the school community understand the need to report inappropriate access even if accidental. (Child to teacher / adult to head teacher)
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns (either on CPOMs / head teacher records).
- 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.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT support (AGILE) are 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.
- Reporting the monitoring of filtering to the Headteacher on a monthly basis.

All staff members are 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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedures.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to the 'Home-School Agreement' in particular aspects relating to online safety and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns to an adult in school or at home.

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 deputies where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

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

- Staff receive regular training
- 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
- Pupils are taught to question information that they encounter when they are online
- Parents are kept up to date with ways in which they can take actions to keep children safe when online

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 Child Protection and Safeguarding Policy.

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, e.g. the Staff Code of Conduct, Low Level Concerns Policy and Disciplinary procedures and disciplinary rules. If the concern is about the head teacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL or DDSL, who investigates concerns with relevant staff members in line with school policies.

Where there is a concern that illegal activity has taken place, the head teacher will contact 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. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by staff on CPOMs in consultation with the DSL. The DSl monitors CPOMs on a daily basis.

Further details of how staff should handle on-line safety procedures can be found in the 'Staff Acceptable Use of ICT Policy' including actions staff should and should not take to protect themselves.

4. Cyberbullying

Example of cyberbullying may include the following:

- Threatening, intimidating or upsetting text messages including those sent in group chats
- Threatening or embarrassing pictures and video clips sent via mobile phone
- 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
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively in line with the 'Anti-bullying Policy.

5. Child-on-child sexual abuse and harassment

The internet and technology can be used as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school as well as off and online. Staff 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 sexualised imagery

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.

The school responds 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 are reported to the DSL, who will investigate the matter in line with the Child Protection, Safeguarding Policy and Behaviour Policy.

6. External influences

Staff need to be aware that, through the internet, children can be exposed to a variety of negative external influences including grooming, child sexual exploitation (CSE), child criminal exploitation (CCE) and radicalisation. Staff should be aware of warning signs of these negative external influences. These might include;

- Being secretive about how they are spending their time.
- 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.
- Changes in the normal behaviour of the child

Where staff have a concern about a pupil relating to pupils' online activity, they will report this to the DSL without delay, who will handle the situation in line with the school Safeguarding, Child Protection and Prevent policies

7. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem.

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. Concerns about the mental health of a pupil will be dealt with in line with the Mental Health and Wellbeing policy.

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 consider the response needed which may include talking to the children about the concern in an age-appropriate manner, seeking further advice and/ or contacting parents.

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, 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 DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils in school cannot

access sites or areas of the internet that may encourage them to stray from lawful use of technology.

10. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. 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.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy the Child Protection Policy and Safeguarding Policy.

11. Online safety and the curriculum

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

- Computing (enhanced through the use of Purple Mash)
- RSE
- PSHE

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 (including an awareness of 'fake' news)
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate.

The risks pupils may face online are always considered when developing the curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC.

The school will consider taking 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 or in response to other events happening on a local or national level.

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

During an online safety lesson or activity, the class teacher ensures 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 Child Protection and Safeguarding 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 Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras
- Learning platforms

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

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

13. Use of smart technology

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.

The school recognises that pupils unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way that breaches the school's 'Acceptable use agreement'. Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers
- Showing indecent images whether consensual and non-consensual
- Viewing and sharing pornography and other harmful content

Pupils will be educated on the acceptable and appropriate use of personal devices but will not be allowed to use these devices on the school premises or a school trip. If a child brings a device into school, it will be stored in the school office until the end of the school day. Pupils are also not allowed to bring smart watches into school that have the capability to link to the internet or take photos.

14. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Home School Agreement at the start of each school year and are encouraged to go through this with their child to ensure their child understands the document.

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. This will be done via newsletters and information provided on the school website.

15. Internet access

Staff are only granted access to the school's internet network once they have read and signed the Acceptable use of ICT Policy and Social media policy.

16. Filtering and monitoring online activity

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. This is provided by Agile. The headteacher ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the head teacher on a monthly basis who manages the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software (ESET), are kept up-to-date and managed by ICT support (AGILE). Firewalls (Smoothwall) are switched on at all times. ICT support review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

All members of staff have their own unique usernames and passwords to access the schools' systems.

Users have their own username and password to access relevant parts of the network suited to their professional position.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the SBM.

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

18. Emails

Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use of ICT Policy. Personal email accounts are not permitted to be used on the school site.

Pupils are taught how to identify suspicious email attachments as part of the curriculum provision.

19. Social networking

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Staff adhere to the school's Social Media Policy.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Behavioural Policy, Low Level Concerns Policy and Staff Code of Conduct Policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Social Media Policy. The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access the school's social media accounts.

All communication on official social media channels by staff on behalf of the school will be clear, transparent and open to scrutiny.

20. The school website

The head teacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. This is monitored by the governing body on an annual basis

21. Use of devices

School-owned devices

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets or laptops to use during lessons. Laptop devices may also be leant to identified pupils to assist with the completion of home learning. Parents/ carers and pupils have to complete a laptop agreement before these are issued.

ICT support (AGILE) review all school-owned devices on an annual basis to carry out software updates and ensure there is no inappropriate material or malware on the devices.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Procedure and Disciplinary Rules and Behavioural Policy respectively.

Personal devices

Any personal electronic device that is brought into school is the responsibility of the user. Pupils are not allowed to use these while in school and staff will use personal devices in school in line with the acceptable use of ICT Policy.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils. Photos and videos of pupils will be taken using school equipment.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

22. Remote learning

All remote learning is delivered in line with the school's Teaching and Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

23. Monitoring and review

The school recognises that the online world is constantly changing; therefore the governing board, headteacher and SBM will monitor this policy regularly in line with the school monitoring plan.

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

Appendix 1

Hatch Warren Junior ICT Acceptable Use Agreement / E-Safety Rules

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep all of my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit internet sites that I know to be prohibited by the school.
- The messages I send on the Purple Mash or Seesaw platform and the information I upload will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher or a responsible adult.
- Messages I send will be kind and I understand that they are part of my digital footprint.
- If I am aware of any cyberbullying, I will notify a trusted adult either at home or at school.

I have read and understand these rules and agree to them.