



Online Safety Policy

Person responsible for the policy	<i>Michelle White</i>
Date approved	<i>June 2026</i>
Approved by	<i>BMC</i>
Review date	<i>June 2027</i>

Contents

Section	Page
Statement of intent	3
1. Legal framework	3
2. Roles and responsibilities	4
3. Managing online safety	6
4. Cyberbullying	7
5. Child-on-child sexual abuse and harassment	7
6. Grooming and exploitation	8
7. Mental health	9
8. Online hoaxes and harmful online challenges	9
9. Cyber-crime	9
10. Online safety training for staff	10
11. Online safety and the curriculum	10
12. Use of technology in the classroom	11
13. Use of smart technology	11
14. Working with parents	12
15. Internet access	12
16. Filtering and monitoring online activity	12
17. Network security	13
18. Emails	13
19. Social networking	14
20. The school website	14
21. Use of devices	14
22. Remote learning	15
23. Monitoring and review	16

Appendix	Title	Page
A	Online harms and risks – curriculum coverage	17
B	Pupil Technology Acceptable Use Agreement	24
C	Staff Technology Acceptable Use Agreement	26
D	Visitor Technology Acceptable Use Agreement	32
E	Volunteer, Work Experience and College Placement Technology Acceptable Use Agreement	34
F	Staff AI Use Agreement	36
G	Filtering and Monitoring Policy	37

The school's ICT provider is currently Easi-PC.



Statement of intent

Hopping Hill 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, suicide, 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 developed this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. A further intention of this policy is to raise awareness of issues concerning cyber security, and the measures implemented also address this area of risk.

1. Legal framework

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

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Keeping Children Safe in Education – current statutory guidance, including any updates when published
- Working Together to Safeguard Children
- DfE Filtering and Monitoring Standards for Schools and Colleges
- DfE Plan Technology for Your School service and related self-assessment tools, where appropriate
- DfE Digital and Technology Standards for Schools and Colleges, including cyber security standards
- DfE guidance on generative artificial intelligence, data protection and safe use of technology in education
- Harmful online challenges and online hoaxes, DfE
- Teaching Online Safety in Schools, DfE
- Searching, Screening and Confiscation, DfE
- Sharing nudes and semi-nudes: advice for education settings working with children and young people, UKCIS
- Education for a Connected World, UK Council for Internet Safety
- Prevent Duty guidance
- When to Call the Police: Guidance for Schools

This policy operates in conjunction with the following school policies and agreements:



- Safeguarding Policy
- Acceptable Use Agreement
- Data Protection Policy
- Anti-Bullying Policy
- Relationships, Sex and Health Education (RSHE) Policy
- Staff Code of Conduct
- Positive Behaviour Policy
- Disciplinary Policy and Procedures
- Pupil Remote Learning Plan
- Filtering and Monitoring Policy – Appendix G
- Staff AI Use Agreement – Appendix F
- Technology Acceptable Use Agreements for pupils, staff, visitors, volunteers, work experience and college placements – Appendices B–E

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 Designated Safeguarding Lead (DSL)'s remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring that online safety, filtering and monitoring, cyber security, data protection and emerging technology
- risks, including artificial intelligence, are considered within safeguarding governance.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding training, including online safety, at induction.
- Accessing termly online safety updates provided by the DSL, including the school picture of concerns, filtering and monitoring activity, any significant issues identified through checks, and actions arising annual online safety and filtering and monitoring audits.
- Ensuring that there are appropriate filtering and monitoring systems in place and clear lines of accountability for the management of this.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding , online challenges.

The headteacher 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 computing subject lead 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.
- Ensuring the school has systems in place to engage parents with online safety that keep them up to date with current issues and how the school is supporting children to stay safe online.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Providing strategic and operational leadership for online safety across the school, ensuring a consistent approach to policy, practice, staff training, incident response, curriculum coverage, filtering and monitoring, and reporting to governors.



- 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 and school business manager.
- 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.
- Working closely with the police during police investigations.
- Keeping up to date with current research, legislation, and online trends.
- Working with the computing subject lead on the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- 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.
- Working alongside the ICT technicians and school business manager to ensure filtering and monitoring tools are age-appropriate, responsive to risk and aligned with current trends.
- Carrying out and recording half-termly filtering checks with another appropriate adult, using a test pupil account across a sample of school devices, including PCs, laptops and iPads, and in different areas of the school.
- Sharing actions from the annual online safety and filtering and monitoring audit with governors and monitoring progress through safeguarding governance arrangements.
- Reporting to the governing board about online safety on a termly basis.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technicians 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.
- Working alongside the DSL and school business manager to ensure filtering/monitoring tools are age appropriate, responsive to risk and aligned with current trends.

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 including local and school community risks.
- 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.
- Using artificial intelligence only in line with the school's Staff AI Use Agreement, including using Microsoft Copilot as the school-approved AI system for school-related work and never using public or non-approved AI tools with personal, sensitive, confidential or identifiable information.
- Reporting online safety, filtering and monitoring, data protection, cyber security or AI-related concerns promptly and not assuming that someone else has already reported them.

Pupils are responsible for:

- Adhering to the Acceptable Use 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 computing subject lead and the headteacher where appropriate.

The school recognises that emerging technologies, including artificial intelligence, can create additional safeguarding risks. These may include misinformation, disinformation, manipulation, impersonation, deepfakes, AI-generated images or videos, bullying, coercion, grooming, image-based abuse, generated harmful content and the inappropriate use of pupil, staff or family information. Concerns involving AI or emerging technology are treated as safeguarding concerns and must be reported to the DSL without delay.

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

- Staff receive regular training.
- Staff receive updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted on the topic of remaining safe 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 Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening. Staff should also be aware that children may disclose abuse gradually, rather than all at once.

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, and appropriate support provided to the victim. The DSL will always act in the best interests of the child or young person.

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. If the concern is about the headteacher, it is reported to the chair of governors.

Details for the chair of governors can be obtained from the school office or through the clerk to the governors using the email address clerk@hoppinghill.northants.sch.uk

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

Where there is a concern that illegal activity has taken place, the headteacher or DSL 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, manage such cases in line with the Safeguarding Policy and refer to *When to Call the Police: Guidance for Schools and Colleges and the National Police Chiefs' Council Guidance 2020*.

All online safety incidents and the school's response are recorded on MyConcern following discussion between the DSL and the staff member to whom the concern was first reported.

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 sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse
- AI-generated or digitally manipulated sexualised images, videos or deepfakes, including content that is fabricated or altered but still causes harm.

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.

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 Safeguarding Policy, the Acceptable Use Agreement, and the Staff Code of Conduct.

Staff must not intentionally view, copy, print, share, store or save nude, semi-nude, sexualised or AI-generated sexualised imagery of pupils, as this may involve a criminal offence. If a pupil shows such imagery to a member of staff

before they can prevent this, the member of staff must stop viewing it as soon as possible, must not ask to see it again, and must report the concern immediately to the DSL. The DSL, in consultation with the headteacher where appropriate, will decide any further action, including whether advice or a referral to children's social care or the police is required.

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 Safeguarding 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, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- 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.
- 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, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

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.

Sextortion is a form of online abuse where someone tricks, threatens or blackmails a child or young person into sending sexual images or videos. Offenders then often pretend to be someone else, and they demand things such as money or further images.

Where staff have any concerns about pupils with relation to CSE or CCE, or sextortion, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding 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, as outlined in the Safeguarding Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. They will also be made aware of the local risks.

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 Safeguarding Policy.

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, and suicidal ideation. 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 Computing subject lead and/or 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 follow advice given by the LA online safety officer. In circumstances where the LA online safety officer is not available and a response to a harmful online challenge or hoax needs to be made quickly, the DSL and/or 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, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- 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 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 even to individual children 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. Parents will be informed where this is assessed as appropriate, taking into account the nature of the risk, the pupils affected, the need to avoid increasing exposure to harmful content, and the school's safeguarding responsibilities.

9. Cyber-crime

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

Cyber-enabled – these crimes can be carried out offline; however, are made easier or more widespread through use of the internet e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.

- **Cyber-dependent** – these crimes can only be committed using computers, networks or the internet. Examples include creating or spreading malware, illegal hacking and booting (flooding a network or system with traffic to make it crash)

The school will factor into its approach to online safety the risk that pupils with a strong interest or ability 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, the DSL will consider contacting the Cyber Choices Programme for advice which supports young people at risk of committing cyber-crime and encourages safer, lawful use of digital skills.

The DSL, headteacher and computing subject lead will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly, and legally. Measures are in place to prevent access to illegal or harmful parts of the internet using school devices and networks including filtering and firewalls.

10. Online safety training for staff

The DSL ensures that all safeguarding training for staff includes relevant aspects of online safety. All staff also complete annual cyber security training and data protection training. Training includes staff responsibilities for keeping information secure, recognising phishing or suspicious activity, protecting personal and sensitive data, using school systems appropriately, understanding filtering and monitoring responsibilities, and reporting any data protection, cyber security, online safety or AI-related concerns without delay. All staff will be made aware that:

- Pupils may be at risk of abuse or exploitation by their peers or by adults.
- Abuse can happen in person and concurrently via digital platforms, e.g. social media and messaging apps.
- Online safety training also covers current online risks, such as:
- Online sexual harassment and grooming.
- Cyberbullying.
- Exposure to harmful content, e.g. self-harm and extremism.
- Sextortion and scams targeting children and young people.

This training is updated regularly to reflect emerging risks and the current picture of reported incidents in school, including AI-generated content, misinformation, deepfakes, online scams, sextortion, cyberbullying, grooming, harmful online challenges and risks identified through Securly alerts or safeguarding records.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum and supported by the online harms and risks curriculum coverage overview in Appendix A; however, it is particularly addressed in the following subjects:

- Relationships, Sex and Health Education (RSHE) / Personal, Social, Health and Economic Education (PSHE)
- Health Education
- PSHE
- Computing
- Digital Literacy

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

The DSL is involved with the development of the school's online safety curriculum. Pupils will discuss 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.

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. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils 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 review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to support the delivery of certain aspects of the online safety curriculum. The computing subject lead and DSL will decide when it is appropriate to invite external groups into school and will ensure that visitors are suitable, appropriately checked, and used in line with the school's external speaker and visitor due diligence procedures, as set out in the Safeguarding Policy.

The DSL will advise staff members on how to best support any pupils who may be especially impacted by online safety lessons. Lessons and activities are 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 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 judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will speak to the DSL and follow the 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 procedures in the Safeguarding Policy.

12. Use of technology in the classroom

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

- Laptops
- Tablets
- PCs

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 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 in school.

13. Use of smart technology



Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Pupil Technology Acceptable Use Agreement in Appendix B.

Staff will use all smart technology and personal technology in line with the Staff Technology Acceptable Use Agreement in Appendix C and the Staff Code of Conduct.

The school will consider the 4C's (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. **Working with parents**

The school endeavours to work in partnership with parents to support pupils in staying 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 Pupil Technology Acceptable Use Agreement in Appendix B at the beginning of each academic year 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 to promote online safety, including but not limited to:

- Ways they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.
- Current issues and risks in online safety.
- Online use that promotes wellbeing and positive mental health.
- How to seek support and help.
- How to talk to their children about online safety and online use, and how to manage incidents of unsafe use.

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

- Class Dojo
- Online resources
- School website
- Monthly newsletters
- Homework is provided termly to pupils in Years 3 to 6, and during the summer term to pupils in Years 1 to 2, to inform parents of curriculum coverage and support discussion with their children.

15. **Internet access**

Pupils, staff, volunteers, visitors and other members of the school community are only granted access to the school's internet network, school technology or guest Wi-Fi where appropriate and once they have read and agreed to the relevant Technology Acceptable Use Agreement, as set out in Appendices B–E. The pupil agreement is made available to pupils and parents at the start of the academic year. Staff agree to the staff agreement through the school's agreed system. A record is kept of users who have been granted guest Wi-Fi access.

The internet is accessed on school devices using the school network and is subject to the school's filtering and monitoring arrangements. Staff, volunteers and visitors must not use personal mobile data or personal internet connections to bypass the school's safeguarding expectations or access, view, download, upload or share anything illegal, harmful, offensive or inappropriate on school premises.

Visitors who are given access to guest Wi-Fi must follow the Visitor Technology Acceptable Use Agreement in Appendix D. Volunteers, work experience students and college placements must follow the relevant Technology Acceptable Use Agreement for their role in Appendix E.

16. **Filtering and monitoring online activity**

The school uses Securly as its filtering and monitoring provider. Securly filtering and monitoring is used to help prevent access to illegal, harmful and inappropriate content and to support the identification of pupils who may be at risk of

harm. Filtering and monitoring support, but do not replace, staff vigilance, supervision, education, professional judgement and safeguarding procedures. Further detail is set out in the Filtering and Monitoring Policy in Appendix G.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, curriculum needs and the risks identified through safeguarding records. Filtering is intended to block illegal, inappropriate and potentially harmful content, including content in different formats such as text, images, video and AI-generated content where technically possible.

The DSL, with another appropriate adult, carries out half-termly filtering checks using a test pupil account across a sample of school devices, including PCs, laptops and iPads, and in different areas of the school. These checks are recorded and used to confirm that filtering is working appropriately across relevant devices and locations. Any concerns identified are followed by the school business manager, headteacher and ICT provider as appropriate.

Requests regarding making changes to the filtering system are directed to the DSL or school business manager working alongside the headteacher. Any changes made to the system are recorded automatically on the Securly Dashboard. Reports of inappropriate websites or materials being accessible are made to the DSL or school business manager, who will work with the ICT provider immediately to investigate the matter and make any necessary changes.

Filtering and monitoring alerts are sent by Securly in real time to the DSL/deputy headteacher, school business manager and headteacher as appropriate. Alerts are reviewed and triaged by trained staff, with human oversight used to assess context, severity and credibility. Where an alert indicates a safeguarding concern, this is recorded on MyConcern and managed in line with the Safeguarding Policy. The DSL analyses alerts and recorded concerns for patterns and takes action where needed, including considering the needs of vulnerable groups.

If a member of staff has deliberately breached the filtering system, they will be considered in line with the Disciplinary Policy and Procedure. However, actions taken will depend on the nature of the breach.

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 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 DSL who manages the situation in line with the Safeguarding Policy.

The school completes an annual strategic review of filtering and monitoring arrangements with input from the DSL, headteacher, school business manager, ICT provider and governors as appropriate. This review considers technical effectiveness, safeguarding impact, checks across devices and locations, alert response, curriculum access, staff training and any actions required. Actions arising from the school's wider annual online safety audit, including but not limited to filtering and monitoring, are shared with governors and monitored through safeguarding governance arrangements.

The annual review may include use of the DfE Plan Technology for Your School service or other appropriate self-assessment tools to support evaluation and identify any required improvements.

17. **Network security**

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

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 ICT technicians.

All members of staff have their own usernames and passwords to access the school's systems. Pupils in Years Reception to 4 have a personal username and use a communal password. Pupils in Years 5 and 6 have a unique username and private password created by the ICT technician. Staff members and pupils are responsible for keeping their passwords private.

Users inform ICT technicians if they forget their login details or if there is a breach, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not 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 is informed and decides the necessary action to take.

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

Staff must use school-approved systems for school-related work and must not enter personal, sensitive, safeguarding, SEND, medical, assessment, behaviour, attendance, family or HR information into public or non-approved AI tools.



Microsoft Copilot is the school-approved AI system for school-related work where AI use is appropriate and permitted by the Staff AI Use Agreement in Appendix F.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement. Staff and pupils 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 Agreement. Personal email accounts must not be used for school-related matters. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are 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 and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails will be identified by the technician who will notify the school. The technician will provide advice, and school will inform the Data Protection Officer (DPO) where necessary.

19. Social networking

Personal Use

Access to social networking sites is filtered as appropriate. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct and Acceptable Use Agreement contain information on the acceptable use of social media – staff members are required to always follow these expectations.

Staff should not use personal social media accounts to communicate with pupils, parents or governors about school matters. Where staff have an existing personal relationship with a parent or governor outside school, they must maintain professional boundaries and must not use personal social media to discuss pupils, school business or confidential matters.

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

Concerns regarding the online conduct of any adult member of the school community on social media are reported to the DSL or headteacher and managed in accordance with the relevant policy.

Use on behalf of the school.

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 is clear, transparent, and open to scrutiny.

20. The school website

The headteacher 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.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

21. Use of devices

School-owned devices

Staff members may be issued with the following devices to assist with their work:

- Laptop
- Tablet



- School mobile phones for specific staff
- PC

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. use during lessons. School-owned devices are used in accordance with the Device User Agreement. All school-owned laptops are password protected.

ICT technicians review all school-owned devices regularly to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

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

Personal devices

Personal devices are used in accordance with the relevant Technology Acceptable Use Agreement and Staff Code of Conduct. Any personal electronic device brought into school is the responsibility of the user.

Staff members are not permitted to use personal devices when working with children unless this is necessary in an emergency or has been agreed by the headteacher or another senior leader for a specific identified reason. Staff members must not use personal devices to take photographs, videos or audio recordings of pupils, staff, parents or school activities.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Safeguarding Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and appropriate action will be taken.

Pupils are not permitted to use personal devices during school time. This includes smart watches that can access the internet, take photographs, record audio or video, or send messages. Devices should be switched off and stored safely by staff. Staff will collect devices at the beginning of the school day, including on entry to the classroom or breakfast club, and return them at the end of the school day, including when pupils leave the classroom or after-school club. Some pupils may have access to a phone or device for agreed medical purposes.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements, and rules for conduct for this are developed and managed on a case-by-case basis.

If staff suspect a pupil is using their device not in line with the Acceptable Use Agreement, they will refer this to the headteacher or Deputy Head/SLT and the device may be searched, screened and confiscated. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Appropriate information is provided to visitors, volunteers, work experience students and college placements regarding the expected use of personal or professional devices. They must follow the relevant Technology Acceptable Use Agreement. Any concerns about the use of personal devices on the school premises are reported to the headteacher, deputy headteacher or DSL.

22. Remote learning

All remote learning is delivered in line with the school's Pupil Remote Learning Plan.

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 DSL, ICT provider, school business manager and headteacher review online safety, filtering and monitoring arrangements to evaluate their effectiveness and ensure they remain appropriate, proportionate and responsive to emerging risks.

The governing board, headteacher and DSL review this policy in full on an annual basis and following significant online safety incidents or changes in statutory guidance. The DSL reports termly to governors on the school's online safety picture, including patterns from online safety concerns, filtering and monitoring activity, any significant issues identified through checks, and actions arising from the annual online safety and filtering and monitoring review.

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

Appendix A: Online harms and risks – curriculum coverage

[The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about.]

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship

	• Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online • How to measure and check authenticity online • The potential consequences of sharing information that may not be true	• General curriculum
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake URLs and websites • What secure markings on websites are and how to assess the sources of emails • The risks of entering information to a website which is not secure • What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship

	be used by fraudsters • What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How cookies work • How data is farmed from sources which look neutral • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship

Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
------------------	---	---

Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done • The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship • General curriculum
-----------------------------	--	---

How to stay safe online

Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
--------------	--	---

Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship

Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not or may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour • The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship

Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely • That online behaviours should mirror offline behaviours and that this should be considered when making a livestream • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship

Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to ‘unrealistic’ online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • That ‘easy money’ lifestyles and offers may be too good to be true • The issue of photo manipulation, including why people do it and how to look out for it	
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum areas: • PSHE • Computing • Digital Citizenship
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online)	This risk or harm is covered in the following curriculum areas: • PSHE

	and how that can lead to pressures around having perfect or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	• Computing • Digital Citizenship
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	

Appendix B: Pupil Technology Acceptable Use Agreement

Hopping Hill acceptable use agreement KS1

At Hopping Hill Primary School, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.



I will:

- ✓ Only use technology when a teacher says I can.
- ✓ Use technology for my learning.
- ✓ Ask for help when I am unsure.
- ✓ Look after the device carefully.
- ✓ Tell an adult if something is not working or damaged.
- ✓ Tell an adult if I see something that makes me feel worried or upset.
- ✓ Tell an adult if someone is not using technology safely.



I will not:



- Share my password with anyone.
- Share my name, age and where I live online.
- Take photos of myself or my friends on school devices.

I understand:

- 👍 I need to use technology safely.
- 👍 An adult can see what I am doing on school devices to keep me safe.
- 👍 If I see something strange or a warning, I will stop and tell an adult.
- 👍 I should do my own work (even when using helpful tools like AI).
- 👍 AI tools can be helpful, but they do not always get things right, so I will think carefully and ask an adult if I am unsure.

My promise:

- ✏️ I will follow these rules when I use technology at school.

Name: _____ Date: _____

Hopping Hill acceptable use agreement KS2

At Hopping Hill Primary School, we know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.



I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and not damage it.
- ✓ Tell the teacher or other adult in class if my device is not working or damaged.
- ✓ Tell the teacher or other adult in class if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher or other adult in class if I see something online that I think is inappropriate or that makes me unsafe or uncomfortable.

I will not:

- ✗ Tell another pupil my username and password.
- ✗ Share personal information, such as my age and where I live, about myself or my friends online.
- ✗ Take photos of myself or my friends using a school device unless an adult tells me to as part of my learning.

Please read each statement and provide a tick to show that you agree to follow these rules all of the time, then write your name below.

I understand why it is important to use technology safely and correctly.



- ☐ I understand my responsibilities when using technology.
- ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- ☐ I understand that everything I do on school devices and the internet in school can be seen and monitored by adults to help keep me safe. If I see a warning or something unusual appears on my screen, I will stop what I am doing and tell an adult straight away.
- ☐ I understand that AI tools can be used to help with learning, but I must think carefully about what they tell me because AI can make mistakes, give false information or include misinformation. I will not copy AI work as my own, and I will never type in private or personal information about myself, my friends, my family or anyone at school.

Name: _____

Date: _____



Appendix C: Staff Technology Acceptable Use Agreement

Staff Technology Acceptable Use Agreement

Technology is an important part of school life and must be used safely, responsibly and appropriately. Misuse will be taken seriously, reported to the headteacher and followed up where necessary. This agreement explains your responsibilities. Please read it carefully and speak to the DSL or headteacher if you have any questions. It has been reviewed in line with Keeping Children Safe in Education (KCSIE) 2026, particularly in relation to filtering and monitoring, emerging technologies and staff safeguarding responsibilities.

1. Using technology in school

- I will only use ICT systems approved for my use by the headteacher, such as a PC, laptop, or tablet.
- I will only use school-approved email accounts for school matters.
- I will delete chain letters, spam or emails from unknown sources without opening them.
- I will check the suitability and reliability of teaching materials from unapproved sources before using them.
- I will not search for, view, download, upload or share harmful, illegal or inappropriate material, including content that may present a safeguarding risk, such as exploitation, grooming or extremist content. If this material appears on any device, including through pop-ups or accidental searches, I will report it to the DSL, headteacher or school business manager.
- I will not install any software onto school ICT systems unless instructed to do so by the school business manager, IT provider or headteacher.
- I will ensure that any alerts on school-owned devices regarding anti-virus software are passed on to the IT provider.
- I will ensure I lock screens on devices when I am not monitoring them.
- I understand that the school uses filtering and monitoring systems to safeguard pupils. I will respond appropriately to alerts or concerns and follow safeguarding procedures, including reporting to the DSL.
- I will not share sensitive personal data unless consent has been given or it is necessary for safeguarding reasons. I will seek advice from the DSL or headteacher if I am unsure.
- I will store personal data in line with UK GDPR and the Data Protection Act 2018.
- I will not share school-related passwords with pupils, staff or third parties unless the leadership team or school business manager has given permission.
- I will only store sensitive or confidential data on removable media or devices when needed to print or scan documents. I will delete it immediately afterwards, including from printer memory.
- Data will be stored on approved school systems. Log in details will be provided to you for this purpose.
- I will use generative AI tools, such as AI chatbots or image generators, responsibly and in line with school AI protocols.
- I will not take, use or store any images or videos of pupils, staff, or parents on any school device unless consent has been sought from the individual(s) in the images or videos, or their parents or carers.
- I will delete all the above from school devices as soon as they have been used for their purpose.

2. Mobile devices

- I will only use school-owned mobile devices when working with children.



- So that I can access my personal mobile device in an emergency, I will keep it secure and safely stored on my person or close to my working area. I will only use it near children during school hours when necessary, in an emergency unless given permission to do so by the headteacher or other senior leader for a specific identified reason.
- I will ensure that my personal mobile devices are set to silent mode during school hours.
- Mobile devices will never be taken into areas where intimate care is taking place.
- I will not use personal mobile devices to take photographs or videos of pupils or staff while in school or involved in school activities such as trips.
- If I use my personal device to access school information or school systems, such as school email or My Concern, I will ensure the device is secure. This includes not saving passwords or using secure access such as facial or fingerprint recognition where available. I will log out after use, and ensure information is not visible to others.
- I will not access or store safeguarding or sensitive pupil information on personal devices unless this has been explicitly authorised and secured in line with school procedures.
- I will not use smart watches online, camera, call or messaging functions when with children. Using a smart watch as a timer or alarm, for example, would be acceptable.

It is impossible to list every situation where staff may need to depart from aspects of the mobile device agreement for safety reasons. Staff should use a common-sense, safety-first approach. If a staff member acts in good faith to maintain safety, this would not be considered a breach.

When taking children off site, staff may use personal mobile phones to contact each other, the school and other necessary people or agencies.

There are circumstances when staff members will have their personal mobile phone in use as a matter of routine. This will be agreed with the headteacher.

3. Social media and online professionalism

- If I represent the school online, for example on a school social media account, I will remain neutral and will not disclose confidential information or post anything that may affect the school's reputation.
- I will only use school-approved accounts and agreed methods to communicate with pupils or parents, such as school email.
- I will never communicate or interact with pupils through personal social networking sites. This includes comments, messages, follows, tags, likes or any other contact on my personal accounts. If a pupil comments on, posts on or otherwise interacts with my open or personal account, I understand that it is my responsibility as the adult to address this once I am aware. I will not reply, will take reasonable steps to prevent further interaction, such as adjusting privacy settings or blocking the account, and will report this to the headteacher or DSL.
- I will not communicate with parents over personal social networking sites unless I have a personal friendship with them. Any such communication must be about non-school matters only.
- I will not give my personal online details to parents unless a personal friendship is already in place.
- Some staff may be friends with parents outside school. Unless communication is through school systems, it must not relate to school matters or take place on school devices.
- I will not accept 'friend requests' or 'follow requests' from any pupils or ex pupils who are not adults (at least 18 years old)
- I understand that I am responsible for my online behaviour, privacy settings and identifying information, both inside and outside school. My online activity must not bring the school into disrepute or raise concerns about my suitability to work with children. Concerns may be addressed by the headteacher through the staff code of conduct, low-level concerns procedures or other relevant school procedures.



- I will not post or upload any defamatory, objectionable, copyright-infringing or private material online, including images or videos of pupils, staff or parents.

4. Working from home (for employed staff)

- I will adhere to the principles of the UK GDPR when working from home.
- I will ensure no unauthorised persons, such as family members or friends, access school devices.
- I will log out of school systems when using personal devices or devices without password protection, such as school tablets. Secure access, such as facial or fingerprint recognition, must be for my use only.

5. Training

- I will complete any online safety training I am directed to undertake and remain up to date with current developments in social media and the internet.
- I will support the DSL and computing lead with regular audits to identify any online safety training needs.
- I will model good practice for pupils when using the internet and digital devices.
- I will deliver online safety learning to pupils as required.

6. Reporting misuse

- I will follow any monitoring responsibilities assigned to me, as outlined in the Online Safety Policy.
- I will report any adult breach of this agreement to the headteacher.
- I will follow the online safety and safeguarding policies if I become aware of pupils' online activity that may be a safeguarding concern.
- I will report concerns about online behaviour, content or safeguarding risk even if I am unsure, and will not assume someone else has reported it.
- I understand that while I am logged on to the school's network or internet service, including on school devices at home, my browsing history may be seen by the headteacher, deputy headteacher/DSL and school business manager. They will receive notifications for blocked usage and will follow up concerns where needed.
- I understand that the school's filtering and monitoring procedures and roles, including A1 protocols, are outlined in a separate document and I will adhere to these at all times.
- I understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

Reviewed June 2026 by Michelle White DSL and DHT

- Staff will sign to show agreement and understanding via My Concern.



Appendix D: Visitor Technology Acceptable Use Agreement

Visitor Technology Acceptable Use Agreement

Please read and sign this agreement when you arrive at school. It explains how visitors must use technology, mobile phones and online access safely while on site.

While visiting the school, I agree that:

- I will only use school technology or internet access if I have been given permission by a member of staff.
- I will follow any instructions given by school staff about safe and appropriate technology use.
- I will not try to access, view, download, upload or share anything illegal, harmful, offensive or inappropriate.
- I understand that the school filters and monitors use of its network, internet and devices to help keep children safe.
- I understand that guest Wi-Fi access must be requested from the school and will only be provided where appropriate. The school keeps a record of who has been given guest Wi-Fi access.
- I will not use my own mobile data or personal internet connection while on school premises to access, view, download, upload or share anything illegal, harmful, offensive or inappropriate, or to bypass the school's safeguarding expectations.
- I will keep my mobile phone and personal devices on silent and will not use them around children unless agreed by a member of the school leadership team or in an emergency.
- I will not take photographs, videos or audio recordings of pupils, staff, parents or school activities unless I have clear permission from the school.
- I will not share any pupil information, images or school-related information online or with anyone outside school unless this is a necessary part of my role and has been agreed by a member of the school leadership team.
- I will not contact pupils through personal email, messaging, social media or online platforms.
- I will report anything that worries me, including unsafe online behaviour, inappropriate content or a safeguarding concern, to a member of school staff immediately.
- I understand that if I do not follow this agreement, the school may withdraw my access to technology or ask me to leave the site.

Visitor declaration

I have read and understood this agreement and agree to follow it while visiting the school.

Name: _____

Organisation / reason for visit: _____

Signature: _____ Date: _____



Appendix E: Volunteer, Work Experience and College Placement Technology Acceptable Use Agreement

Volunteers, Work Experience and College Placements Technology Acceptable Use Agreement

Please read and sign this agreement before starting in school. It is for volunteers, work experience students and college placements who do not have their own school login. Student teachers or adults given access to school accounts must follow the staff acceptable use agreement instead.

While in school, I agree to the following:

- I will only use school technology, guest Wi-Fi or the internet in school if I have permission from a member of staff.
- I understand that I will not normally have access to the school network, school systems or a school login.
- If I am given access to guest Wi-Fi, I understand that my internet use will be filtered and monitored.
- I will follow staff instructions about safe and appropriate use of technology.
- I will not try to access, view, download, upload or share anything illegal, harmful, offensive or inappropriate.
- I will not try to install apps or software, change settings, bypass filtering, or use websites or apps that have not been allowed by the school.
- I will not use, ask for, or share anyone else's login details.
- I will keep my mobile phone and personal devices silent and away while I am with pupils or in pupil areas.
- I will only use my phone or personal device during breaks or lunchtime, in staff-only areas, or away from pupils if I need to take an essential call.
- I will not use my own mobile data or personal internet connection to bypass the school's safeguarding expectations.
- I will not take photographs, videos or audio recordings of pupils, staff, parents or school activities unless the school has clearly given permission and this will never be using a personal device.
- I will not store, post or share images, personal information or anything about pupils, staff or the school unless this has been agreed by a senior member of staff.
- I will not contact pupils through personal email, messaging, social media, gaming platforms or other online accounts.
- I will report anything that worries me, including unsafe online behaviour, inappropriate content or a safeguarding concern, to a member of school staff straight away.
- I understand that, where appropriate, the school may share concerns about unsafe, inappropriate or harmful behaviour with relevant people or agencies, such as my college, placement provider, parents/carers, the local authority or the police.
- I understand that if I do not follow this agreement, the school may remove my access to technology or end my placement.

Volunteer / Placement declaration

I have read and understood this agreement and agree to follow it while working or volunteering in the school.

Name: _____

School / College / Reason for placement: _____

Signature: _____ Date: _____

Reviewed June 2026 by Michelle White, DSL and DHT



Appendix F: Staff AI Use Agreement

Hopping Hill Primary School: Staff AI Use Agreement

Purpose: This agreement outlines the responsible use of artificial intelligence (AI) tools by staff at Hopping Hill Primary School to support teaching, learning and administrative tasks, while ensuring compliance with safeguarding expectations, data protection legislation and KCSIE 2026 guidance. School staff should use Microsoft Copilot as the school-approved AI system. Other AI tools may be used for school-related work where no personal, sensitive, confidential or school-identifiable information is entered or uploaded.

1. How to Use AI

- AI can support teaching, learning and administrative work, but it must be used carefully and in line with the school's rules on permitted tools and information safety. Staff must follow the guidance in this agreement before using AI for school-related tasks.
- AI is a support tool, not a substitute for staff judgement. It must not replace professional knowledge, lesson planning decisions, assessment, safeguarding procedures or responsibility for the final content shared with pupils, parents or colleagues.
- Staff must check AI-generated information for accuracy, relevance and age-appropriateness before using it or sharing it with pupils, parents or colleagues.

2. Keeping Information Safe

- Microsoft Copilot is the only permitted AI tool for school-related work involving internal, personal, sensitive, confidential or identifiable information.
- Staff must access Microsoft Copilot using their school Microsoft account when using it for school-related work.
- Sensitive information should not routinely be entered into Microsoft Copilot. Any use of sensitive information with Copilot must be necessary, appropriate and approached with caution.
- Public or non-approved AI tools must never be used with information that could identify the school or a person in the school community. This includes, but is not limited to, pupil, parent, staff, assessment, report, SEND, medical, behaviour, attendance, safeguarding, family or HR information.
- If you are unsure whether information is suitable to use with AI, do **not** upload it. Ask the DSL/headteacher for guidance first.

3. Writing Reports with AI

- If AI is used to support report writing, staff must use Microsoft Copilot.
- You must review, edit and adapt all AI-generated report content so that it reflects your professional judgement and knowledge of the child.
- Reports must be personalised, accurate and appropriate. AI must not be used to replace teacher assessment, professional judgement or safeguarding decision-making.

4. Safeguarding and Safe Use

- You must never use any AI tool to make safeguarding decisions, assess risk, diagnose need, predict pupil behaviour or decide whether a concern should be recorded or referred. Safeguarding concerns must always follow the school's safeguarding procedures.
- If AI produces inappropriate, harmful, misleading or unsafe content, or if you are concerned that AI has been misused, you must report this to the DSL/headteacher immediately.
- You must be aware that AI can present safeguarding risks, including misinformation, manipulation and generated content such as fake images.
- Staff should take appropriate opportunities to raise pupils' awareness of the risks, benefits and limitations of AI, and model safe, responsible and realistic expectations about how AI may be used in everyday life.
- You must access and engage with any AI, safeguarding, data protection or online safety training and guidance provided by the school.



5. Copyright and Ownership

- Staff must not assume that AI-generated content is copyright-free or safe to copy.
- Staff should take reasonable steps to check that AI content does not copy or closely imitate published material, such as text, images, worksheets, websites or commercial resources.
- AI-generated resources must be reviewed and adapted before being used or shared. If there is doubt, the content should not be used without further advice.
- Resources created using AI for school purposes should be treated as school materials and stored, shared and used in line with school expectations.

Reviewed June 2026



Filtering and Monitoring Policy

2025-2026

EasiPC

01604 286682

info@easipc.co.uk

28 Quarry Park Close, Northampton NN3 6QB

Microsoft in
Education Global
Training Partner





Appendix G: Filtering and Monitoring Policy

1. Introduction and Aims

This policy outlines the principles, procedures, and guidance for filtering and monitoring internet access at **Hopping Hill Primary School**. Our primary commitment is to safeguard and promote the welfare of our students, providing a safe online environment where they can learn and thrive.

The aims of this policy are:

- To protect students and staff from illegal, harmful, or inappropriate online content.
- To enable access to appropriate online resources that support effective teaching and learning.
- To identify and support students at risk of online harm through proactive monitoring and clear intervention processes.
- To ensure the school's IT systems are used responsibly and for educational purposes.
- To educate students on how to stay safe online and become responsible digital citizens.

2. Policy Context and Statutory Obligations

This policy is written in line with our statutory duties and is guided by key legislation and advice, including:

- **Keeping Children Safe in Education (KCSIE):** Schools must "have appropriate filtering and monitoring systems in place" and review them annually.
- **DfE Digital and Technology Standards:** Sets the expectation that schools should have compliant and effective systems to "filter and monitor what users can access."
- **The PREVENT Duty:** Requires schools to have due regard to the need to prevent people from being drawn into terrorism, which includes blocking terrorist content and monitoring for online radicalisation.
- **The Education Act 2002 / Independent School Standards:** Requires schools to safeguard and promote the welfare of children.

3. Scope of the Policy

This policy applies to all internet and network use on systems provided by the school. Its scope covers:

- **School Network and Devices:** All devices owned by the school, and all users accessing the internet through the school's wired or wireless networks.
- **School-Managed Devices Off-Site:** School-owned devices (e.g., student laptops) used outside the school premises. Filtering and monitoring on these devices remain active at all times.
- **Bring Your Own Device (BYOD):** Any personal device (laptops, tablets, phones) connected to the school's guest Wi-Fi network. These devices are subject to the same level of filtering as school-owned devices, though the school's ability to monitor activity may be limited.
- **Staff and Visitor Use:** All staff, volunteers, contractors, and visitors using the school's internet



access are subject to this policy.

4. Roles and Responsibilities (Summary)

- **Governing Body/Proprietor:** Has overall responsibility for ensuring the school meets its statutory duties regarding online safety.
- **Headteacher and Senior Leadership Team (SLT):** Responsible for the implementation of this policy, ensuring staff are appropriately trained, and for the strategic oversight of the systems' effectiveness.
- **Designated Safeguarding Lead (DSL):** Takes lead responsibility for all safeguarding matters, including managing the response to monitoring alerts and leading the operational review of the systems.
- **IT Support/Technical Staff:** Responsible for the technical maintenance and configuration of the filtering and monitoring systems.
- **All Staff:** Responsible for promoting online safety and reporting concerns.

5. Filtering Policy

Hopping Hill Primary School uses **Securly Filter** to block access to harmful and inappropriate content. Our approach is to make the learning environment safe without unreasonably restricting curriculum access.

- **Compliance:** The system blocks access to illegal content as defined by the Internet Watch Foundation (IWF) and the Counter-Terrorism Internet Referral Unit (CTIRU).
- **Age-Appropriateness:** Filtering levels are customised for different year groups. Policies are reviewed to ensure they are not overly restrictive and meet educational needs.
- **Technical Components:** Filtering is enforced on all school-managed devices, both on and off-site, using the **Securly SmartPAC** client or **Securly Chrome Extension**.

6. Monitoring Policy

Our approach to monitoring is founded on proactive safeguarding. **Hopping Hill Primary School** uses **Securly Aware** to identify students who may be at risk of harm.

- **Principles:** Monitoring is purposeful, proportionate, transparent, and secure. It is a tool for intervention and support, not surveillance.
- **Scope of Monitoring:** Monitoring is performed on school-managed systems, including web browsing, emails, chats, and documents within the school's **Microsoft 365** tenancy.
- **Alert and Triage Process:**
 1. **Automated Detection:** Securly Aware AI flags content indicative of risk.
 2. **Initial Alert & Triage:** An alert is sent to a designated team led by the **DSL**.
 3. **Risk Assessment (Human Oversight):** A trained staff member reviews the context to assess the severity and credibility of the concern.
 4. **Action and Intervention:** The DSL determines the appropriate, proportionate response



based on the assessed risk.

5. **Recording:** All actions are recorded in the school's safeguarding records.

7. The Role of Education and the Curriculum

Technology alone is not a solution. Our approach to online safety is a combination of **Technical Controls, Education, and Policy**.

- Filtering and monitoring are tools that complement, but do not replace, the education of students.
- Online safety is taught as an integral part of the **PSHE**, Computing, and RSE curriculum.
- Students are taught how to stay safe online, think critically about content, and how and when to report a concern.
- Staff receive regular training on online safety as part of their safeguarding updates.

8. Responding to Incidents and Breaches

8.1. *Process for Requesting Access to Blocked Content*

We recognise that filtering systems may occasionally block legitimate educational resources. Staff can request access using the following procedure:

1. **Request:** The staff member emails the IT Support desk with a link to the resource, providing a brief educational justification. The staff member also informs the DSL to ensure they are confident with the resources in their safeguarding capacity.
2. **Review:** The request will be reviewed by IT Support and the DSL to ensure the resource is appropriate and safe.
3. **Action:** If approved, the resource will be added to the 'allow list' (whitelisted). The staff member will be notified of the outcome. We will aim to respond to all requests within **[e.g., 24 hours]**.

8.2. *Responding to Breaches of this Policy*

Any attempt to bypass the filtering and monitoring systems or to access, create, or transmit inappropriate material will be taken seriously. Breaches of this policy will be handled in line with the school's **Student Behaviour Policy** or **Staff Disciplinary Policy**. Responses may include, but are not limited to, a discussion with the student/staff member, restricting IT access, informing parents/carers, and, where illegal activity is identified, informing the police.

9. Management and Strategic Review

The school is committed to a robust and regular review of its filtering and monitoring provision to ensure it remains effective, compliant, and fit for purpose.

The detailed procedures, agenda items, and reporting structure for this process are documented in the school's separate **Filtering and Monitoring Review Template**.



9.1. Frequency and Scope of Review

- **Frequency:** An operational review of the filtering and monitoring systems will be conducted **at least termly**. A full, strategic review of this policy and the systems' overall effectiveness will be completed **at least annually**, in line with KCSIE guidance.
- **Scope:** The scope of the review is to assess the systems' technical performance, their effectiveness in safeguarding students, their impact on teaching and learning, and to ensure all related processes are being followed correctly.

9.2. Responsibility for Review

The review process is led by the Designated Safeguarding Lead (DSL) and includes oversight from the Senior Leadership Team (SLT), input from the IT Support Lead, and accountability to the Safeguarding Governor. The specific roles, responsibilities, and attendees for the review meetings are detailed in the **Filtering and Monitoring Review Template**.