

Abbots Hall Primary Academy



Online Safety Policy

Approved by Governors: September 2026

Signed: _____ Date: _____

Policy to be reviewed: September 2027

Designated Safeguarding Lead (DSL)	Jack Arnold – Headteacher
Deputy Designated Safeguarding Lead (DDSL)	Stuart Holmes – Deputy Headteacher
Named person for safeguarding	Dawn Smith – Family Support Worker
Designated safeguarding Governor	Rita Garner – Chair of Governors
Computing Lead	Amy Coe

Version control

Date	Version no.	Key changes from previous version
11/18	V1	New policy
3/20	V2	SWGFL Model Policy Links to Curriculum planning tools References online radicalisation Data Protection information Changes to personnel References to relevant
7/2/22	V3	Updated key personnel Alteration to action taken over issues published in 'behaviour policy', to 'published policies' Student owned devices allowed in school where school requests – in line with remote learning.
9/25	V4	Wholesale change of policy
9/26	V5	Substantive changes to reflect changes to KCSIE including: filtering and monitoring, roles and responsibilities, terminology, mobile devices.

Contents

Abbots Hall Primary Academy	1
1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	6
5. Educating parents/carers about online safety	8
6. Cyber-bullying	8
7. Acceptable use of the internet in school	10
8. Pupils using mobile devices in school	10
9. Staff using work devices outside school	11
10. How the school will respond to issues of misuse	11
11. Training	11
12. Monitoring arrangements	12
13. Links with other policies	13
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	14
Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)	15
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)	16
Appendix 4: online safety incident report log	17
Appendix 5: Incident report flowchart	16

1. Aims

Our school aims to:

- › Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- › Identify and support groups of pupils that are potentially at greater risk of harm online than others
- › Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- › Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate harmful online interactions; for example, peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes.
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, including images generated using artificial intelligence, consensual and non-consensual sharing of nudes and semi-nudes, and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff](#)
- › [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- › Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- › Reviewing filtering and monitoring provisions at least annually
- › Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- › Having effective monitoring strategies in place that meet the school's safeguarding needs

The governor who oversees online safety is Rita Garner

All governors will:

- › Make sure they have read and understand this policy
- › Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- › Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- › Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- › Ensure that the school has appropriate filtering and monitoring systems in place and that their effectiveness is reviewed at least once every academic year.
- › Ensure a member of SLT undertakes an annual review that will include checks that filtering is working appropriately on **all internet-connected devices in all relevant locations** used by pupils and staff. A written record of these checks, including any issues identified and actions taken, will be retained by the school.
- › Receive appropriate assurance that the review has been completed, that identified concerns have been addressed and that relevant staff understand the filtering and monitoring arrangements and how to escalate concerns where problems are identified.

3.2 The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL), Deputy DSL, Named person for safeguarding and Safeguarding Governor are set out in our Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the school's ICT Support (BIS Solutions) to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT Support and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT Support (BIS Solutions)

The ICT Support is responsible for:

- Supporting the member of the Senior Leadership Team responsible for filtering and monitoring and the DSL with the annual review of filtering and monitoring arrangements, including testing that filtering is working appropriately on **all internet-connected devices in all relevant locations** used by pupils and staff.
- Providing evidence of the checks undertaken, including any failures, weaknesses or inappropriate blocking identified and the action taken to address them, so that the school can retain a record of the annual review. Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Understanding their role and responsibilities in relation to filtering and monitoring, including how to report concerns where filtering or monitoring appears to have failed or is not operating as expected. Concerns should be reported promptly through MyConcern and escalated to the DSL or ICT Support as appropriate.
- Following the correct procedure of emailing ICT Support if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, and specifically in Computing and PSHE lessons. The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

All schools have to teach:

- [Relationships education and health education](#) in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- › Use technology safely and respectfully, keeping personal information private
- › Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- › Use technology safely, respectfully and responsibly
- › Recognise acceptable and unacceptable behaviour
- › Identify a range of ways to report concerns about content and contact
- › Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- › That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- › That people sometimes behave differently online, including by pretending to be someone they are not
- › That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- › The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- › How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- › How information and data are shared and used online
- › How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- › What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- › How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- › The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- › Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- › How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- › Where and how to report concerns and get support with issues online

As part of the school's preventative education programme, pupils will receive age and stage-appropriate teaching about emerging and developing online harms.

This will include, where appropriate to the age and developmental stage of pupils:

- the risks associated with sharing images and videos online, including the making and sharing of nudes and semi-nudes;
- the prevalence and potential harms of deepfakes and other artificially generated or manipulated content;
- the risks associated with pornography and exposure to sexualised content online;
- the influence of misogynistic and other harmful online content and influencers;

- how online content can present a distorted picture of real life and may normalise or glamorise behaviours which are unhealthy, harmful or wrong;
- how to critically assess information and distinguish between reliable information, misinformation and disinformation; and
- when, where and how to seek help and report concerns about online harms.

Teaching will be adapted to ensure that it is appropriate to pupils' age, stage of development and individual needs, including the needs of pupils with SEND and other vulnerabilities.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website, ClassDojo or monthly newsletter. This policy will also be shared with parents/carers via the school website.

Where relevant, online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's class teacher.

Concerns or queries about this policy can be raised with any member of staff.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of the Senior Leadership Team (SLT) authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or deputy headteacher
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher or Deputy Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, authorised staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects that a pupil has made, received, possessed or shared a nude or semi-nude image or video, including an image or video that has been digitally altered or generated using artificial intelligence, they must not view, copy, save, print, forward or otherwise distribute the image or video.

The device should be confiscated where appropriate and the incident reported to the DSL or deputy DSL immediately.

All incidents involving the making or sharing of nudes or semi-nudes, including where the sharing appears to have been consensual, will be treated as a safeguarding matter and assessed by the DSL in accordance with the school's safeguarding procedures and the latest DfE and UKCIS guidance.

The DSL will determine the appropriate response, including whether advice or referral to children's social care, the police or another relevant agency is required.

Where an image may constitute evidence of an offence, it must not be deleted or further distributed and the DSL will seek appropriate advice.

This approach applies equally to images that are wholly or partly generated using artificial intelligence, including deepfakes or so-called deep nudes.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)

- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The Behaviour Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Abbots Hall recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We treat any use of AI to bully pupils very seriously, in line with the anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should request permission from a member of the Senior Leadership Team before doing so. Before permission is given, a risk-assessment must first be carried out.

AI-generated content will be considered within the school's wider online safety and safeguarding arrangements. This includes artificially generated or manipulated images, audio or video, including deepfakes and AI-generated nudes or semi-nudes.

The school will respond to AI-related safeguarding concerns in the same way as other online safeguarding concerns and will consider the potential impact on both the child affected and any child who has created or shared harmful content.

Pupils will be taught, in an age and stage-appropriate way, that content generated or manipulated using AI may appear realistic but may not be genuine, and that they should seek help if they encounter harmful or concerning AI-generated content or interactions.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. The DSL team receive daily filtering reports outlining any websites or searches that have been blocked.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Abbots Hall Primary Academy is a mobile-phone-free environment by default.

Pupils must not have access to mobile phones during the school day, including during lessons, the time between lessons, breaktimes and lunchtime.

Children who bring a mobile phone to school are required to switch the phone off and hand it to their class teacher on arrival. The phone will be stored securely until the end of the school day and returned to the pupil at the agreed collection time.

Pupils are not permitted to wear smart watches or use any device with connectivity or a camera unless an exception has been specifically authorised by the school because of an identified need.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from ICT Support (BIS)

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse other children online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of nudes and semi-nudes, including AI-generated imagery, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL, DDSL and named person for safeguarding will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

11.2 Pupils

Through the curriculum, all pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- The risks of social media platforms, live streaming and online gaming
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The Named person of safeguarding logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5. Online safety logs will be monitored by the DSL Team each month.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board.

The Named Person for Safeguarding logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 4. Online safety logs will be monitored by the DSL team regularly and reviewed formally at least monthly.

The school will undertake a formal review of its online safety provision at least annually, supported by an annual risk assessment that considers and reflects the online risks faced by pupils.

Filtering and monitoring

The school will ensure that appropriate filtering and monitoring systems are in place on school devices and networks.

At least once during each academic year, the member of the Senior Leadership Team responsible for filtering and monitoring will lead a review of the effectiveness of the school's filtering and monitoring arrangements, with support from the Designated Safeguarding Lead and ICT Support.

The annual review will include checks that filtering is working appropriately on **all internet-connected devices in all relevant locations** used by pupils and staff.

A written record of these checks will be retained by the school. The record will identify the date of the review, those involved, the devices and locations checked, any issues identified, and any actions taken to address those issues.

The review will also consider whether:

- harmful and inappropriate content is blocked without unreasonably impacting teaching and learning;
- monitoring strategies remain appropriate to the school's safeguarding needs;
- relevant staff understand the filtering and monitoring arrangements;
- staff know how to report and escalate concerns;
- the arrangements remain proportionate to the age and needs of pupils; and
- the systems continue to reflect the risks identified through the school's safeguarding and Prevent risk assessments.

The outcome of the annual review will be reported to the governing board as part of its safeguarding oversight.

This policy will be reviewed at least annually by the DSL in consultation with the relevant member of the Senior Leadership Team and ICT Support. It will also be reviewed sooner where there are significant changes to legislation, statutory guidance, technology, filtering or monitoring arrangements, or emerging online safeguarding risks.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- PSHE Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I select a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for educational activities only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the usernames and passwords I have been given
- Try my hardest to remember my usernames and passwords
- Never share my passwords with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Only save my work on the school network when an adult asks me to.
- Check with my teacher before I print anything
- Log off or shut down a computer or other device when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or trusted adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive or inappropriate
- Log in to someone else's personal account
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will turn it off when I enter the school gates.
- I will hand it in to my class teacher until the end of the day.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 5: Incident report flowchart

