Online Safety Policy

Review frequency:	Annually
Last reviewed:	March 2025
Agreed by Directors:	26/03/25
Next review date:	March 2026

Introduction:

The internet is an essential tool in 21st century life for education, business and social interaction. Therefore, we have a duty to provide our children with quality internet access as part of their learning experience. Online Safety is a crucial part of this internet world and encompasses Internet technologies and electronic communications such as mobile technology and wireless technology. Most young people are enthusiastic internet users - particularly of interactive services like: chat, gaming, vlogging and streaming via apps. However, like many exciting activities, there are risky situations to deal with and hazards to avoid.

Aims:

It is the aim of this school to educate our children about the benefits and risks of using new technologies and how to be able to safely control their own online experiences. We will do this by:

- ➔ Having robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- ➔ 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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behavior that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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
- Relationships and health education

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 programs of study.

Roles and Responsibilities:

The ***Standards Committee*** has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. They will:

- ➔ coordinate meetings with appropriate staff to discuss online safety, and monitor online safety concerns as provided by the designated safeguarding lead (DSL)
- ➔ Ensure that they have read and understood this policy
- ➔ Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- ➔ Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- ➔ Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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 they are giving support where appropriate e.g., additional resources, training and time for the headteacher to fulfil this role

The ***Headteacher (and Designated Safeguard Lead)*** is responsible for:

- ➔ ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- ➔ Working with Network Manager/ICT Service Provider 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 child protection policy
- ➔ Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ➔ Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behavior policy
- ➔ Updating and delivering staff training on online safety
- ➔ Liaising with other agencies and/or external services if necessary
- ➔ Providing regular reports on online safety in school to the headteacher and/or governing board
- ➔ ensuring that the school has appropriate filtering and monitoring on school devices and school networks.

This list is not intended to be exhaustive.

The ***Network Manager/ICT Service Provider***

is responsible for:

- ➔ Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ➔ Ensuring 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 yearly
- ➔ monitoring the school's ICT systems on a daily basis
- ➔ Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ➔ Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- ➔ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behavior policy

This list is not intended to be exhaustive.

All ***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 and ensuring that pupils follow the school's terms on acceptable use
- ➔ Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ➔ Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behavior 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'
- ➔ Being aware that Internet traffic will be monitored and traced to the individual user. Discretion and professional conduct is essential
- ➔ Safe use of digital images and digital technologies, such as mobile phones, digital cameras, tablets and iPads
- ➔ Using a safe search engine when accessing the Internet on a school device, (e.g. Google Safe Search).

This list is not intended to be exhaustive.

Parents/Carers are expected to:

- ➔ Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- ➔ Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

Educating children about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- ➔ Relationships education and health education in primary schools

In **Key Stage 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 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behavior
- Identify a range of ways to report concerns about content and contact

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

- ❖ 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 online 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 is shared and used online
- ❖ 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 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.

Educating Parents about online safety:

The school will raise parents' awareness of internet safety in letters, newsletters and/or other communications home, as well as via our website and Facebook page. This policy will also be shared with parents. Parents will be given a copy of the Acceptable Use Agreement for their child to sign. They will be encouraged and supported to monitor their children's use of technology at home.

The school will let parents know:

- ➔ What systems the school uses to filter and monitor online use
- ➔ 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 have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

Cyber-bullying:

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 one person or group by another person or group, where the relationship involves an imbalance of power.

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 are encouraged to do so, including where they are a witness rather than the victim.

The Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying and the issue will be addressed in assemblies and Digital Citizenship lessons.

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.

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

For more information on the signs of cyberbullying please refer to our Anti-Bullying Policy.

Examining electronic devices:

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the Academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
- Report it to the police

If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence. 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

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

Acceptable use of the Internet in school:

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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.

Pupils Using Mobile Devices in Schools:

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- On the playground, during, before or after school
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. Any breach of the acceptable use agreement by a pupil may trigger

disciplinary action in line with the school behavior policy, which may result in the confiscation of their device.

Staff using work devices outside of 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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- 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
- School devices are for the express use of the individual who has been assigned the device and not for use by anyone else in their household.
- Installing anti-virus and anti-spyware software (to be done by the Network Manager/ICT Service Provider)
- Keeping operating systems up to date by always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- Staff and pupils should not use any external storage device unless it has been provided by the Network Manager/ICT Service Provider.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager/ICT Service Provider.

How the Academy will respond to issues of misuse:

Where a pupil misuses the Academy's ICT systems or internet, we will follow the procedures set out in the behavior policy. 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 Academy'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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

- **Filtering: If staff or pupils discover an unsuitable web site, it must be reported to the Network Manager/ICT Service Provider or ICT STAFF, the screen can be closed but the computer should not be shut down to allow further investigation.**
- The Network Manager/ICT Service Provider will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Our filters send reports of any suspicious searches. These are viewed by the

Network Manager/ICT Service Provider/ICT STAFF and DSL. The DSL will investigate further, if required.

- All staff and pupils know how to report instances of inappropriate computer or internet use and are aware that this must be done immediately. (Staff can report instances of computer or internet misuse to the Network Manager/ICT Service Provider or ICT STAFF, either in person, or through email to a support email address. If this is not possible or the instance is severe the member of staff can go straight to the Head of School/DSL. Pupils can report instances of computer or internet misuse to any member of staff who can then follow the staff process.)
- Changes to the filtering are made by the Network Manager/ICT Service Provider. Any member of staff can request a website to be unfiltered and must provide a reason. This can be done in person, but is recommended that it is requested by email or support ticket with the website listed. The Network Manager/ICT Service Provider will then review the site and check that it is appropriate for educational purposes. If deemed appropriate it will be unfiltered for the relevant filtering policies.
- In line with KCSIE 2023, parents, governors and staff receive information about our filtering systems for in school and for school devices outside of school. We use our termly online safety and computing newsletters to communicate this information and governing body meetings to discuss wider issues concerning online safety.
- Our filtering system relies on daily-updated filter lists from the IWF and Counter Terrorism Policing's CTIRU within the Metropolitan Police Service. This ensures strict adherence to PREVENT guidelines, with monthly updates directly from CTIRU.
- Our filtering provider is officially recognized as an appropriate filtering service by the UK Safer Internet Centre
-
- These comprehensive measures collectively ensure our strict compliance with the revised KCSIE (September 2023) Annex C guidelines.
- **Training:**

- 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, e-bulletins and staff meetings). As part of these sessions, online safety and safeguarding will be included.

- 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 their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, 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 and deputies 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 child protection and safeguarding policy.

Monitoring Arrangements:

The DSL logs behavior and safeguarding issues related to online safety on our Provision Map portal.

This policy will be reviewed every year by a member of the SLT. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links to other policies:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices

- Complaints procedure
- Anti-Bullying

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

- UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-car ers/what-are-issues
- Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Internet Matters: https://www.internetmatters.org /

ThinkUKNow (CEOP) https://www.thinkuknow.co.uk

Key Stage One Acceptable Use Agreement

This is how we stay safe when we use school devices:

- I will ask a teacher or suitable adult if I want to use a device.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of school devices.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a school device.
- I will not share my username and password or any other private information with anyone.

To be completed by a parent/guardian & returned to school:

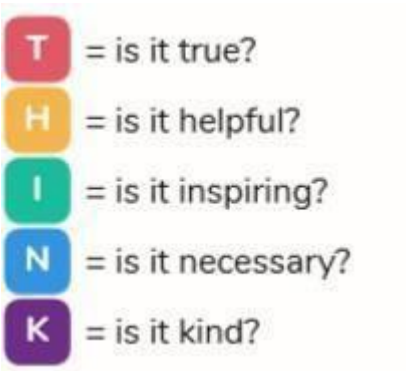
Child's name : _____

Parent/Guardian name: _____

Parent/Guardian signature: _____

Key Stage Two Acceptable Use Agreement

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.



- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken

I understand this agreement and know the consequences if I don't follow it.

My Name: Class:

Parent/Carer Signed: Today's Date:

EYFS Acceptable Use Agreement