Watlington Primary School
Online Safety Policy

January 2024

Next due review: January 2026

Signed: _____ Headteacher Date: January 2024

Gemma Sterjo

Policy has been adopted / reviewed by Governing Body:

Signed: _____ Chair of Governors Date: January 2024

Finbar McGaughey

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, 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 behaviour 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 sex education
- 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.

Roles and responsibilities

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, e-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, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 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 their safeguarding needs.

The governor who oversees online safety is Finbar McGaughey

All governors will:

- Ensure 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)
- 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 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

The headteacher

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

The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure 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
- Working with the ICT technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Logging and managing all online safety issues (see appendix) and incidents in line with the school's safeguarding and child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring 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 headteacher and/or governing board
- Undertaking annual risk assessments (see appendix) that consider and reflect the risks children 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.

The ICT technician

The ICT technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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
- Monitoring the school's ICT systems on a regular basis, as directed by the senior leadership team

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

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 ensuring that pupils follow the school's terms on acceptable use (see appendix)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting this to the DSL and / or Headteacher
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 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'
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Parents/carers

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 (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
- Hot topics – Childnet

- Parent resource sheet – Childnet

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Primary schools insert:

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

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, such as Jigsaw (PSHCE) 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/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. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' information evenings.

The school will let parents/carers 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/carers 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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 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. Class 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 Jigsaw), 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).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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.

Examining electronic devices

The headteacher, and any member of staff 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 / DSL
- Explain to the pupil why they are being searched, 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 other member of the senior leadership team 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 if 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, 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** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident 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

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
- Our behaviour policy / searches and confiscation 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.

Artificial intelligence (AI)

Generative artificial intelligence (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 Bard.

Watlington Primary School 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.

Watlington Primary School will treat any use of AI to bully pupils in line with our anti bullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by Watlington Primary School.

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 (see appendices). 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.

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

Pupils using mobile devices in school

Year 6 pupils may bring mobile devices into school, in order to use if walking home independently. They are stored by the class teacher and children are not permitted to use them during:

Lessons

Break / lunch times

Clubs before or after school, or any other activities organised by the school

Any use of mobile devices by pupils must be in line with the acceptable use agreement (see Appendix).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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 – 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
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- Any USB devices containing data relating to the school must be encrypted, however it is preferable for work to be saved on to the school network.
- They must take all reasonable steps to ensure the security of their work device when using it outside school.

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 the IT Technician.

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 and acceptable use. 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 / staff code of conduct. 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.

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).

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, threatening, 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 behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Headteacher and DSL. At every review, the policy will be shared with the governing board. The review (such as the one available here) 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 with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable use agreement (Primary Pupils)

Acceptable Use Statement

Primary Pupils

Our pupils use school IT systems as part of their learning. To ensure a safe online environment for all, we ask our pupils to respect the following rules:

● I will only use computers and other devices as directed by a teacher.

● If I have been given a username and password I will keep it to myself and not tell anyone else.

● I will use the computers and other devices in a responsible, appropriate and sensible way.

● I am responsible for my behaviour when using the internet. This includes the resources and the language I use.

● I will not look at, download, upload or forward material that could upset others and if I see something that is upsetting or worrying then I will tell my teacher straight away.

● I will not give out my personal information such as my name, phone number or address.

● I will only take and/or use images of pupils and/or staff should only be taken and used when my teacher gives me permission.

● I will ensure that my online activity both in school and outside of school will not cause my school, my teachers or other children distress this includes gaming.

● I will follow the school rules regarding E-Safety.

● I will not copy other people's work.

● I understand that my teacher can see what I do on the computer.

● I understand that these rules will keep me safe and I must follow them.

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

This agreement is designed to ensure that all staff, visitors and Governors are aware of their professional responsibilities when any form of data or ICT is accessed or used. All staff, visitors (where appropriate) and Governors are expected to sign this agreement and adhere to its content.

In signing this document, you agree to the following:

Key principles

● I understand that I must use school systems in a responsible way to ensure there is no risk to my safety or to the safety and security of the system and other users.

● I have read and understood The Acer Trust Data Protection Policy and Privacy Notice and I agree to adhere to its principles and processes.

● I will ensure that data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

● I agree to follow the school's processes for managing data and understand my responsibility for reporting any breach.

General protocols

● I will only use the school's email, internet, intranet and any other learning platforms or technologies for professional purposes or for uses deemed 'reasonable' the Headteacher or Governing body.

● I will ensure that all electronic communications with pupils and staff are related to my role and responsibilities and I will use my school email account for business purposes only.

● Any internal emails that includes data relating to a pupil or staff member must be anonymised (by initials) in the subject header. Highly sensitive information if being sent externally (3rd party) must be sent via encrypted email (such as egress) or password protected.

● Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and consent on school approved devices or personal devices if approved by senior leadership. Images on personal devices should be removed after 5 working days.

● I will not install any hardware or software without the permission of the IT technician

● I will support and promote the schools E-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

● I will password protect any technologies that I use as part of my role and will not share my password with others. I agree to change my password on a regular basis.

Working environment

● I agree to keep all paper documents that contain data secure.

● I will ensure that other adults within school or pupils cannot see or gain access to data in any form - paper or electronic.

● I will shred any documents that contain data if not needed for retention.

● I will retain any paper and/or electronic documents as required by our data policy following the school's systems.

Remote working and off site

● I understand that I can access and use school or pupil data off site (working from home/school trips) and accept it is my responsibility to ensure data is kept secure at all times.

● Personal and sensitive data taken off site or accessed remotely must be encrypted or stored/accessed on a password protected device.

● Any paperwork containing data (for example school trip pupil information) must be signed out and back in and upon return it must be shredded.

● When working at home I understand that I must lock or shut down my device if I ever move away from it. School equipment must not be used by family members.

Professional responsibility

● I will not give out my own personal details, such as mobile phone number and personal email address to any pupils.

● I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

● I will not deliberately upload or add images, video, sounds or text that could upset or offend.

● I will respect copyright and intellectual property rights.

● I will ensure that my online activity, both in school and outside school will not bring my professional role in disrepute.

● I understand that all use of the internet and other technologies can be monitored and logged and can be made available, on request, to my line manager or Headteacher.

● [Staff only] I understand that this forms part of the terms and conditions set out in my contract of employment.

Any person who has access to data or the school's ICT systems (including email) are required to sign this agreement.

Name:_____ Role:_____ To be reviewed and signed annually

Signed_____ Date:_____

Appendix 3: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

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:

Risk Assessment Form						
Location/Dept: **Watlington Primary School**		**Date Assessed:** January 2024		**Assessed by:**  **Jonathan Gale (Deputy Head / DSL)**		
Task/ Activity: **Online Safety**		**Review Date:** January 2025				
Hazard/Risk	**Persons at risk**	**Controls in place**	**Severity (1-5)**	**Likelihood (1-5)**	**Risk/ Priority**	**Additional controls required**
Pupils may use devices to access inappropriate materials online when in school. Pupils may unintentionally be exposed to inappropriate materials online when in school.	Children	Acceptable use agreement to be read and signed by pupils at start of year as part of a lesson on online safety. Acceptable use agreement sent home as part of enrolment pack. Home-school agreement outlines online safety expectations. Instruction on safe behaviour online to be part of the computing curriculum across the school, including safe searching; how to report concerns. Also covered as part of the school's Jigsaw (PSHE) curriculum. Staff to support when internet is being used. Children to be supervised at all times when using online resources in school. Filtering systems in place to prevent access to inappropriate, illegal or harmful sites.	2	3	6	Acceptable use agreements signed by children (whole-class) Home-school agreements shared. Weekly monitoring of Securly monitoring reports by Gemma Sterjo (HT) and Jonathan Gale (DSL), with follow up actions carried out as appropriate. Staff confirm they have read and understood Safeguarding and Child Protection policy on an annual basis.

		Monitoring systems (Securly) in place to support DSL / HT with identifying individuals who have accessed inappropriate content. Links to CEOP / ThinkUKnow etc. shared on school website.				
Pupils may use the device to access inappropriate materials online when learning at home (e.g. when participating in remote learning / completing homework tasks). Pupils may unintentionally be exposed to inappropriate materials online when learning at home (e.g. when participating in remote learning / completing homework tasks).	Children	Home-school agreement outlines parents' responsibilities. Staff check websites and online resources for suitability before directing children to them. When delivering remote learning, staff follow the school's remote learning policy. Links to CEOP / ThinkUKnow etc. shared on school website.	2	3	6	
Pupils may be contacted by strangers when using online communication tools. Pupils may be at risk of: • Cyberbullying • Grooming • Exploitation • Cyber crime	Children	Support and education around safety measures, as part of Jigsaw PSHE / the school's computing curriculum. Pupil's capacity / vulnerability must be risk-assessed. If it is believed they do not have capacity / are too vulnerable to make safe decisions, staff will provide additional support and monitoring. The curriculum will also be adapted to meet children's needs as and when necessary. Staff to ask pupils about how they use the internet, what social networking sites are accessed,	3	2	6	

		what games they play and what apps they have, discussing the potential risks they may be exposed to. Open culture where staff can enquire about pupils' use of online tools and offer support around this. Staff to discuss with student, what to do if someone they have never met face to face, contacts them, or what to do if they see something that worries them. Online safety information shared with parents through safeguarding newsletters / website, providing them with tools and resources for how to discuss online safety with children.				
Pupils may disclose personal data e.g. their name / date of birth / contact information to strangers.	Children	Acceptable use agreement to be read and signed by pupils at start of year. Instruction on safe behaviour online is part of the computing curriculum across the school, including safe searching; how to report concerns. Staff to support when internet is being used. Children to be supervised at all times when using online resources in school. Filtering and monitoring systems in place to prevent access to inappropriate, illegal or harmful sites. Links to CEOP / ThinkUKnow etc.	2	2	4	Weekly monitoring of Securly monitoring reports by Gemma Sterjo (HT) and Jonathan Gale (DSL), with follow up actions carried out as appropriate.

		shared on school website.				
Children may be vulnerable to scams and / or phishing.	Children	Computing / PSHE Jigsaw curriculum informs pupils of what scams and phishing are and risks are explained. Vulnerability to scams/phishing to be considered as part of individual children's risk assessments when necessary. Filtering and monitoring systems in place to prevent access to such content.	2	1	3	Weekly monitoring of Securly monitoring reports by Gemma Sterjo (HT) and Jonathan Gale (DSL), with follow up actions carried out as appropriate.

Distribution List:		**Job Title:**		**Date:**	

Risk/Priority Indicator Key

Likelihood
1 Remote May only occur in exceptional circumstances
2 Unlikely Expected to occur rarely (not expected in the next 12 months)
3 Possible Expected to occur under some circumstances (50/50 chance of occurrence within the next year)
4 Probable Strong chance this will occur within the next year
5 Highly Probable Expected to occur in the next 12 months

Severity (Consequence)
1 Negligible Not a noticeable effect on the school; no injuries; no damage to reputation
2 Minor Limited short-term disruption to operations; minor injuries/illness; small financial loss
3 Moderate Some disruption to operations for 48 hours; short term illness/injuries; some damage to reputation; financial loss that can be managed within budget; potential for adverse publicity – avoidable with careful handling
4 Major Loss of operations for up to a week; severe injuries; severe financial loss with impact on operations; damage to reputation, local press coverage.

RISK / PRIORITY INICATOR MATRIX

LIKELIHOOD						
	5 Highly Probable	5	10	15	20	25
	4 Probable	4	8	12	16	20
	3 Possible	3	6	9	12	15
	2 Unlikely	2	4	6	8	10
	1 Remote	1	2	3	4	5
		1 Negligible	**2 Low**	**3 Moderate**	**4 High**	**5 Extreme**
		SEVERITY (CONSEQUENCE)				

Summary		Suggested Timeframe
12-25	High	As soon as possible
6-11	Medium	Within next 3-6 months

5 Extreme/Catastrophic Loss of operations for more than a week; severe injuries or loss of life; gross failure to meet national/professional standards; major long term consequences; extensive coverage in press; major financial loss that threatens existence.	1-5	Low	Whenever viable to do so

All High and Medium risks must have additional controls put in place to reduce the risk.