Internet Safety Policy

Waltham St Lawrence Primary School

Governors' Committee Responsible	**Full Governing Board**
Status	**Statutory**
Review Cycle	**Annual**
Date Written/Last Review	**September 2026**
Date of Next Review	**September 2027**

Our mission is to provide inspiration and opportunities for all children to achieve their potential and become confident, independent individuals with key skills for lifelong learning

Contents

• The background to this policy
• Rationale
• The online safety curriculum
• Continued Professional Development
• Monitoring, and preventing online safety incidents
• Responding to online safety incidents
• Appendices (including PIC)

Background to this policy:

The purpose of this policy is to describe the safeguarding measures in place for adults and children in Waltham St. Lawrence Primary School in relation to online safety, including:

•The policies and practice embedded in our school and followed by the whole school community
•The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding
to online safety incidents
•A progressive, relevant age-appropriate online safety curriculum for all pupils

Online safety in schools is primarily a safeguarding and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

• Safeguarding and Child Protection
• Personal Social and Health Education (PSHE)
• Data Protection / GDPR Policy
• Anti-Bullying Policy
• School Complaints Procedure
• Whistle Blowing Policy

This policy must be read alongside the Staff and Pupil Internet Charter as attached as appendices. This Charter outlines the expectations and sanctions which apply to staff and pupil use of technology.

The development of our Internet Safety Policy involved

- The Headteacher
- The Designated Safeguarding Lead
- The Computing Subject Leader
- The governor responsible for Safeguarding

This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email and a staff meeting and is readily available on the school network and website, and has also been made available to parents.

All staff must be familiar with this policy and all staff and pupils must sign the relevant Staff and Pupil Internet Charter before being allowed to access school's systems (see appendices). As Online safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Intent:

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. (Teaching Online Safety 2019)

We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

Implementation:
At Waltham St. Lawrence Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

Evaluation:
We want our children to be able to evaluate what they see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

- Questions pupils may ask include:
- Is this website/URL/email fake? How can I tell?
- What does this cookie do and what information am I sharing?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information? What's behind this post?
- Is this too good to be true?
- Is this fact or opinion?

Risks:
The risks they may face can broadly be categorised into the '3 C's' Contact, Content and Conduct (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing ofSelf-Generated Indecent Images
- •The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- AI, unreliable media.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:
Staff:

- Staff laptops, iPads and also desktops in the office and in classrooms.
- Staff / some staff have access to school systems beyond the school building (e.g. MIS systems, cloud storage of school files). Staff devices can also be used at home in accordance with the Staff and Pupil Internet Charter, particularly with regard to GDPR.
- Class cameras. iPads and other peripherals such as visualisers and Interactive Whiteboards
- SMART watches

Pupils:

- Curriculum laptops / iPads / classroom desktops including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (Beebots, Microbits, crumbles, control equipment, class cameras etc.)

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The online safety curriculum:

When using online technologies, it is essential that children understand how to behave in a safe, respectable and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- At KS1: 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.
- At KS2: use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Waltham St. Lawrence Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe
- Practice in our online learning platforms: Purple Mash
- Our programme for online safety education is evidenced in teachers' planning both as discrete, embedded and continuous activities uses the child-led learning platform Purple Mash
- Whole School Internet Safety day
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.

Continued Professional Development:

- All staff at Waltham St. Lawrence Primary School receive up-to-date information and training on online safety issues in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.
- Nominated members of staff and govenors receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.
- New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

School website:

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information our pupils and parents, promote the school to prospective ones and publish as a minimum the statutory information required by the Department for Education.

In conjunction with a range of online services, our school website, which is maintained by SchoolOnline, can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.
Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as it would apply to its physical surroundings. Our Headteacher and the Governing Body therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, information displayed on the school website.
The school has established clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.

Mobile phones and use of 5G data in school:
Keeping Children Safe in Education (2026) highlights the need for schools to have a clear policy statement on, and carefully consider 'how access to 5G data is managed on their premises', and also how they manage the increasing risk of 'peer on peer abuse'.

At Waltham St. Lawrence Primary School, we do not permit pupils to bring mobile phones into school. If in an emergency, the children must give them to the office on arrival who will return them after school. Pupils are also not allowed to use SMART watches to contact or be contacted by anyone using 5G throughout the school day.

Monitoring, and averting online safety incidents:
The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Secure, private RBWM provided internet connection to each school with a direct link to the National Education Network.
- Managed SOPHOS firewalling running Unified threat management (UTM) that provides Restrictions on download of software, apps and file types from known compromised sites.
- Base line and optional enhanced filtering.(updated to Securly August 2025)
- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.
- Antivirus package provided as part of TIO contract
- Email system for all school staff, with any data sent being password protected.
- Wireless networks installed by Turn It On are encrypted to industry best practice standards and the wireless key should be kept securely.
- Staff also monitor pupils' use of technology and, specifically, their activity online.
- Pupils' use of online services (including the World Wide Web) are supervised in school at all times.
- Staff are also able to monitor pupils' activity when using Purple Mash online, allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.
- A system of staff and pupil passwords is in place to enable appropriate access to the school network.
- All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.(where appropriate)
- Visitors to the school can access part of the school systems using a generic visitor login and password. (Wireless)
- The wireless network is encrypted to the standards advised by the Local Authority.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Responding to online safety incidents:
It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident
occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, Waltham St. Lawrence Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's Staff and Pupil Internet Charter – see appendix).
- Initially an incident report must be filled out and stored in Head teacher's office.

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

With this in mind, the Headteacher may decide to apply the sanctions and / or procedures in the Staff and Pupil Internet Charter to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.
However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.
Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed.

Waltham St Lawrence Primary School

Staff and Pupil Internet Charter

We, the staff and pupils of Waltham St Lawrence and our parents/guardians have agreed to this charter covering the expectations we have of using Laptops, Computers, the Internet and any devices that can send or receive online messages.

- At Waltham St Lawrence Primary School we expect to be responsible for our own behaviour on the Internet, just as we are anywhere else in school. This includes materials we choose to access, and language we use.

- We communicate through our Virtual Learning Environment, Purple Mash, where we each have our own email account and class domain.

- We use the World Wide Web and are expected not to deliberately seek out offensive materials. Should we encounter any such material accidentally, we are expected to report it immediately to a teacher.

- We are not to use any rude language in our email communications and contact only people we know or those the teacher has approved. It is forbidden to be involved in sending chain letters.

- We must never use ICT to upset or offend others, if we feel offended we must report it to a teacher.

- We must ask permission before accessing the Internet.

- We should not access other people's files unless specific permission has been given.

- School Laptops and online devices should only be used for schoolwork and homework unless permission has been granted otherwise.

- No program files may be downloaded to the computer from the Internet.

- No programs on disk, memory stick or CD Rom should be brought in from home for use in school unless given to teacher.

- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).

- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

- Any pupil mobile phones brought into School for emergency purposes must be immediately given to the Class Teacher and stored securely.

- Pupils are not allowed to receive or send messages through SMART watches and, if they are worn 5G must be disabled throughout the school day (including any before or after school clubs).

- We understand that. if we choose not to comply with these expectations we will be warned and may be denied access to computing resources.