St Lawrence C of E (Aided) Junior School

	Reviewed	**September 2024**
	Next Review	**September 2025**

Online Safety and Acceptable Usage Policy

Technology has revolutionised the movement, access and storage of information and this has important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate have changed our perception of when and where learning takes place. At St Lawrence, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Online Safety seeks to address the issues around using these technologies safely and to promote an awareness of the benefits and the risks. This is taught discreetly through specific lessons, units of work and themed days (Safer Internet Day) but also as an integral part of each computing lesson or indeed any other lesson where the use of ICT and/or the internet is involved.

This policy sets out clearly our expectations for pupils, staff, parents and members of the wider community to ensure best practice.

Key: Normal text gives contexts and information

Italic text indicates teaching given to pupils.

Bold text indicates key expectation to ensure positive and safe use.

Online Safety - Roles and Responsibilities:

Designated Safeguarding Lead (DSL): Grace MacLean

Senior Leadership Team (SLT): Grace MacLean, Rachel Copsey, Liz Searle

IT Service Provider: Adept Technology Group (ATG)

Online Safety Lead: Stephanie Gould

Governor for Safeguarding: George Cameron

The SLT shall be responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why

- reviewing the effectiveness of our provision
- overseeing reports

The SLT is responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

SLT shall work closely with governors, the DSL and our external IT service providers (ATG) in all aspects of filtering and monitoring.

The DSL shall take lead responsibility for Safeguarding and Online Safety, which shall include overseeing and acting on:

- safeguarding concerns
- filtering and monitoring reports
- checks to filtering and monitoring systems.

The SLT may delegate the implementation of this policy to members of staff or external suppliers or consultants.

ATG shall have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems.

ATG shall work with the SLT and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Online Safety Team

The Online Safety team shall be formed by the DSL, SLT, IT Service Provider and the Online Safety Lead.

1. Physical Safety:

All electrical equipment in the school is tested to ensure that it is safe to use.

Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum.

We expect pupils to behave appropriately near electrical sockets and appliances.

All the projectors in our school have maximum light levels in line with Government Health and Safety guidance.

Pupils are taught that they should not look directly at strong light sources such as the sun, lasers or data projectors.

We expect all users to not look directly into the light beam when working on the interactive whiteboards.

Workstations are cleaned and sanitised regularly.

Pupils are taught to avoid taking food and liquids anywhere near the computers.

We expect all users to refrain from eating and drinking when working at a computer.

Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks.

Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. Administrative staff receive regular Display Screen Equipment training.

We expect all users to take responsibility for their own physical well-being by adopting good practices.

Computers and other ICT equipment can be easily damaged.

Pupils are taught the correct way to use ICT equipment.

We expect pupils to respect ICT equipment and take care when handling and using it.

2. Network Safety:

All users need to log on using a username and password. Pupils log on using their personal username and password.

Pupils are taught that they should only access the network using that particular log in and do not disclose their details to other users.

We expect all users to only logon using their username.

Each user is given an allocation of disk space for the storage of their work.

Pupils are taught how to save their work into their "My documents" area.

We expect pupils to save and keep their work to build up a portfolio of evidence.

Access to other users’ “My documents” areas are restricted by the network.

Pupils are taught not to access another user’s work without permission.

We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user’s work.

On the network there are “shared resource” areas where many different groups of users can save work so that it is available to others.

Pupils are taught how to access and save to these shared resource areas.

We expect pupils to respect the contributions of others, not to delete or alter others’ work and to ensure that they only save work to shared areas with permission.

Each user is given the opportunity to print.

Pupils are taught to print only when necessary in order to save resources for financial and environmental reasons.

We expect pupils to print out work only when directed by staff to do so.

The network software prevents changes being made to computer settings.

Pupils are taught that making changes may prevent the computer from working properly.

We expect all users to make no attempt to alter the way the computer is set up.

Only the network administrators are permitted to install software on to computers.

Pupils are taught that the network or an application may not function properly if programmes are installed.

We expect all users to make no attempt to load or download any programme onto the network.

All users of the network can be monitored remotely by the network administrators.

Pupils are taught that their use of the network can be monitored.

We expect all users to understand that their use is subject to monitoring.

3. Internet Safety: Filtering and Monitoring

To ensure that St Lawrence meets its safeguarding duties, in particular to block harmful and inappropriate content being accessed on the school’s IT systems, the school will ensure that appropriate systems are used to filter internet and other communications and to monitor and report upon the effectiveness of such systems. The school shall: -

• identify and assign roles and responsibilities to manage filtering and monitoring systems
• review filtering and monitoring provision at least annually
• block harmful and inappropriate content without unreasonably impacting teaching and learning
• have effective monitoring strategies in place that meet its safeguarding needs.

Definitions

Filtering: Filtering blocks access to harmful sites and content.

Monitoring: Monitoring identifies when a user accesses or searches for certain types of harmful content.

When using a network workstation all access to the Internet shall be protected by a number of different filters. These filters, which must be based upon industry-standard web filters designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators may additionally block or filter site addresses which are considered to be unacceptable.

Pupils are taught that the Internet contains many websites that are useful but that there are also websites which are unpleasant, offensive, and not child-friendly or which can damage your computer.

We expect pupils to make no attempt to access websites that they know to be unsuitable for children and/or contain offensive language, images, games or other media.

Monitoring

The school expect users to behave responsibly but accepts no system is 100% safe. Acknowledging such expectations may not always be met the school shall monitor the effectiveness of its filtering processes and identify and report upon any breach.

Filtering & Monitoring Checks:
All internet usage and apps on all devices shall be monitored and checked. The DSL shall be responsible for managing the filtering and monitoring systems in the school, working with the IT Service Provider to ensure effective systems are in place.

Daily Monitoring:
All class teachers shall be trained to monitor their pupils when using devises or apps in lesson time. Teachers shall rotate around the room during these sessions monitoring what is happening and shall alert the DSL if there are any concerns.

Half Termly Monitoring:
A review shall be conducted by two members of the Online Safety Team during each half-term period to ensure that filtering and monitoring systems are working effectively. They shall check and confirm that: -

- the filtering is working for all stakeholders as designed,
- the filtering is active everywhere, eg: for all devices and relevant users,
- sites are ‘overblocked’
- any concerns about whether pupils can bypass blocked sites.
- safe searches are turned on and that they cannot be bypassed.

Filtering & Monitoring Annual Audit:

An audit of the school's filtering and monitoring systems shall be conducted on an annual basis by the DSL, Online Safety Lead and IT Service Provider. This annual review shall be reported to the Governing Body.

Breaches of the Filtering and Monitoring Systems

Should an Online Safety breach be identified through the filtering and monitoring systems, the IT Service Provider or other person identifying the breach must notify the DSL as required by the **Child Protection and Safeguarding Policy**

Filtering and monitoring breaches shall be promptly addressed by the DSL where appropriate with the individual and parents, as well as initiating action to minimise Online safety risks.

Out of School Usage

Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities, any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school.

We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.

The school website contains school policies, newsletters and other information.

We expect all persons accessing the school web site to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.

4. Virtual Learning Environment (VLE):

The school provides information through the Virtual Learning Environment (VLE) for children and parents. This is not the sole point of contact for home/school communication and is an aid to children's learning. School may provide homework tasks on the VLE, however understands that some pupils do not have access to this at home.

Pupils are taught how to use the VLE to aid their learning outside of school.

We expect all pupils accessing the VLE to treat the content with respect and use it to further their learning outside of school. Time is set aside in homework club for children to access the VLE if they do not have access at home.

5. Email Safety:

Some pupils will have their own email accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. The use of personal email accounts by pupils at school or at home for school purposes is not permitted.

Pupils are taught that using a personal email account in school or for school use is not permitted.

We expect pupils to use personal accounts responsibly and not during school time.

6. Digital Images:

Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. On the website we never state a child's full name with their image.

The school will remove any image of a child on the school website at their parents' request.

Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff.

Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school.

We expect all pupils to seek permission from staff before sharing images outside the school environment.

7. Bullying (Cyberbullying):

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. This includes, but is not restricted to, the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. St Lawrence accepts responsibility for in-school incidents and incidents associated with internet-based activities set by the school. External incidents which arise are not the school's responsibility.

*Pupils are taught about bullying as part of the PSHE curriculum***.** *School provides a wealth of information to aid adults to improve their knowledge of OnlineSafety.*

We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the whole school policy on Behaviour, including bullying.

Any concerns over online bullying or inappropriate use of the internet can be reported to

admin@stlawrence-junior.surrey.sch.uk

Pupils are taught to report concerns over online bullying or inappropriate use of the internet to a responsible adult.

The school will respond to queries and provide advice and endeavour to resolve the problem.

8. Mobile Phones:

Pupils are not permitted to have mobile phones upon their person in school. We recognise that our pupils may walk on their own to and from school and that parents may wish them to have a mobile phone for emergencies. However we discourage this on security grounds as they are easily lost, damaged or stolen.

Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the class teacher for the duration of the day.

We expect pupils not to carry a mobile phone in school.

9, Other Technologies

Podcasting – Some pupils will be given opportunities to create oral recordings. Some of these recordings may be made available as podcasts through the Internet so that they can be shared with interested members of the local community.

The pupils will not identify themselves by full names or by class, only by year group.

The school will monitor the content and distribution of recorded material.

10. Copyright:

Though there are lots of 'free-to-use' resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances. This is particularly so for music, but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the

Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology.

Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission.

We expect all users to respect copyright laws.

It is important to know what work is original and when passages of text or images have been copied from other sources such as the Internet.

Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information.

We expect all pupils to make it clear what is their own work and what is quoted from other sources.

11. Reporting

It is important that pupils are aware of when and how to report inappropriate use and content of the online facilities within the school and also at home.

Pupils are taught that some websites are not appropriate for children and have suggested age restrictions. Pupils are taught to only access websites that the teachers have given them permission to use. They are taught to close webpages they are not sure about and are provided with strategies for reporting anything they are unhappy with, including content and messages.

We expect all pupils to only access websites they have been given permission to use by an appropriate adult and to report any inappropriate or worrying content or online behaviour.

12. School Online Safety Rules:

These rules will help to keep everyone safe and help us to respect others.

- I will only use the school's computers with permission from an adult
- I will not tell anyone my login or password
- I will only login to the school systems as myself
- I will only edit or delete my own files
- I am aware that some websites and social networks have age restrictions which mean that I must not go on them and I will not use internet chatrooms
- I will only visit internet sites that are appropriate for my age and that an adult has chosen
- I will only communicate with people I know, or that a responsible adult has approved
- I will only send polite and friendly messages
- I will not open an email from anyone I don't know.
- I will not open an attachment, or download a file, unless I have been given permission by an adult
- I will not tell anyone my home address/phone number, send a photograph/ video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet anyone I don't know
- I will immediately close any web page I am not sure about.
- If I see anything I am unhappy with or I receive a message I do not like, I will show a responsible adult.
- I understand that the school may check my computer files and the internet sites I visit.
- I understand that if I deliberately break these rules, I will not be allowed to use the internet or computers.

Glossary of Terms

Email: text based messages sent through the Internet
Internet: a global network of computers which allow efficient communication from any point to any point
Network: a group of computers linked together and often managed by a server
Podcast: one of a series of sound files uploaded onto the Internet and downloaded by subscribers. **Server:** a computer that controls access to a network or computers and usually stores data for all users.
Webmail: email service which is held on a secure website and can be accessed anywhere on the Internet.