William Austin Infant School

Online Safety Policy

January 2025

Scope of the Policy

This policy applies to all members of the *school* (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the *school.*

The purpose of this policy is to:

- To ensure the safety and wellbeing of our children and staff is paramount when adults, young people or children are using the internet, social media or mobile devices.
- To provide staff and volunteers with the overarching principles that guide our approach to online safety.
- To ensure that, as an organisation, we operate in line with our values and within the law and guidance in terms of how we use online devices.
- To clearly identify and assign roles and responsibilities to manage filtering and monitoring systems as outline in Keeping Children Safe in Education 2024.

Our Online Safety Policy has been written by the school, building on the LSCB Online Safety Policy, NSPCC model policy and government guidance. This policy has also been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. It has been agreed by senior management and approved by governors

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

All children will follow a programme of study for Online Safety based on project Evolve which uses the government framework: Education for a Connected World (2018.)

Project Evolve covers the following 8 areas of Online Safety:

- Self Image and Identity
- Online Relationships
- Online Reputation
- Online Bullying
- Managing Online Information
- Health, Well Being and Lifestyle
- Privacy and Security
- Copyright and Ownership

Why is it important to teach our children about the internet and digital communications?
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

How will using the Internet enhance learning and how do we keep the children safe?
The school Internet access is designed expressly for pupil use and includes filtering from Netsweeper that is appropriate to the age of our pupils. Our monitoring system is provided by Senso which records and monitors both staff and children's internet use on school devices at school and when using them off site.

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught how to report unpleasant internet content to members of staff and this will be dealt with accordingly.

Online safety messages should be reinforced when introducing and using Email with pupils, including:

- Keeping passwords safe and private (not telling others our passwords)
- Writing kind messages
- Always logging out of accounts
- Never logging on to another person's account
  Pupil image file names will not refer to the pupil by their full name. First name or initials should be used.
  Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Remote Learning due to a school closure or pupil isolating.
Messages are to only be sent to the school staff member by a parent via school email addresses

All staff when using video communication whether live or pre-recorded must:

- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programmes as intended.
- Not record, store, or distribute video material without permission.
- Always remain aware that they are visible.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents via email about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Managing Internet Access
The School ICT systems security will be reviewed regularly by the Computing Lead, Partnership Education and members of SLT.

Virus protection will be updated regularly.

A log for malware is kept by the ICT technicians who are provided by Partnership Education.

Information system security
Pupils may only use approved e-mail accounts on the school system such as 2email on Purple Mash.

Offensive e-mails are automatically blocked (based on offensive words) and sent to the administrator's account. These are then dealt with accordingly.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The forwarding of chain letters is not permitted.

Staff or pupil personal contact information will not generally be published.

Staff are given work email accounts to use for the sole use of work related emails and these, not personal email accounts, should be used for all school based communication.

Published content and the school web site
The contact details given on our website are of the school office.

The Headteacher, Computing coordinator and Office Administrator will take overall editorial responsibility and ensure that content is accurate and appropriate however Staff have a responsibility to ensure that all content waiting to be uploaded to the school website is factually accurate and that only children with photo permission are present in photos.

Publishing pupils' images and work
A variety of multimedia, including photographs, videos, and sound clips that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs rather than full-face photos of individual children should be used.

Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school website. Written permission will initially be obtained when children start school.

Parents have the option to request whether or not children's photos are used on our school website and staff are aware of children whose images are not to be shared. Written consent must be given to change this and stored in a central location accessible to all staff who would use photos of children on display or on the website. Work can only be published with the permission of the pupil and parents/carers. Pupils' photos will be retained and/or remain published no more than 2 years after they have left the school.

Staff sign the school's Social Media and Internet Acceptable Use Policy and Code of Conduct this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.

Managing emerging technologies
Emerging technologies will be examined for educational benefit before use in school is allowed.

The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by pupils of cameras in mobile phones will be kept under review.

Staff will be issued with a school phone where contact with parents/carers is required or where mobile phones are used to capture photographs of pupils.

The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;

The school's Broadband Internet settings identify staff logins and filters appropriately.

Social Networking and personal publishing
The school will control access to social networking sites, and consider how to educate pupils in their safe use.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Social networking sites will not be accessible by children using school equipment.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering
The school works with Netsweeper and Senso to ensure systems are in place to protect pupils. These are reviewed regularly and improved when needed.

If staff or pupils come across unsuitable online materials, the site must be reported to the Lead Teacher for Computing and an email sent to itsupport@williamaustininfants.co.uk for the attention of the IT Technician.

Senior staff ensure that regular checks are made to ensure that the filtering and monitoring methods selected are appropriate, effective and reasonable. The Lead Teacher for Computing, Headteacher, Chair of Governors and IT technician take overall responsibility for checking that filtering and monitoring is appropriate.

Managing videoconferencing & webcam use
Videoconferencing should use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and General Data Protection Regulation (GDPR).
It is made clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.

Handling Online safety complaints
Complaints of internet misuse will be dealt with by a senior member of staff.
Any complaint about staff misuse must be referred to the Headteacher in accordance with the school's Social Media and Internet Acceptable Use Policy Whistleblowing, Code of Conduct and Low Level Concerns policy.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (The Luton Online Safety Policy has a flowchart of responses to an incident or concern.)

Pupils and parents will be informed of the complaints procedure (see school's complaints policy)

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Policy Decisions

Authorising Internet access
All staff must read and sign the Staff Code of Conduct and Social Media and Internet Acceptable Use Policy for computing before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1 and EYFS, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

Any person not directly employed by the school will be asked to sign an “acceptable use of school ICT resources” before being allowed to access the internet from the school site.

Assessing risks
The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school, LBC nor the LSCB can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the policy is appropriate and effective.
The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

The school will liaise with local organisations to establish a common approach to online safety.

Staff will regularly receive training updating them on the best way to support children and the issues they may face.

The school has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data.

All computer equipment is installed professionally and meets health and safety standards;

The school fosters a ‘No Blame’ environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable.

The school has a clear, progressive online safety education programme throughout the school.

All children are to be taught the SMART rules and to take part in online safety specific activities as part of Safer Internet Day yearly.

Communications Policy

Introducing the Online Safety Policy to pupils
Online Safety rules will be shared and discussed with pupils regularly and planned across the curriculum as well as in Online Safety Planning.

Pupils will be informed that network and internet use will be monitored and appropriately followed up.

A programme of training in online safety, based on Project Evolve, Education for a Connected World Framework and Think you know online resources, is being used across Early Years Foundation Stage and Key Stage 1.

Online safety training is embedded within the Computing scheme of work.

Staff and the Online Safety policy
All staff will be given the school Online Safety Policy and its importance will be explained.

Staff are informed that network and internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always ensure they pre load websites or use a child friendly safe search engine when accessing the web with pupils.

Staff ensure that when copying materials from the web, both they and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

Community use of the Internet
The school will liaise with local organisations to establish a common approach to Online Safety.

Enlisting parents' and carers' support
Parents' and carers' attention will be drawn to the School Online Safety policy in newsletters, the school brochure and on the school website. Resources will be accessible through the school website as well as in newsletters.

The school provides online safety advice for pupils, staff and parents. Parent workshops will be run yearly to keep parents informed with all latest information regarding online safety.

Reviewed: January 2025

Next review: January 2026