William Austin Infant School

Online Safety Policy

January 2026

Scope of the Policy

This Online Safety Policy outlines the commitment of William Austin Infant School to safeguard members of our school community online in accordance with the statutory guidance and best practice. This Online Safety 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.* It also applies to the use of personal digital technology on the school site.

William Austin Infants School will deal with such incidents within this policy and associated behaviour and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of 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 outlined in Keeping Children Safe in Education.

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.

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

- The Headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
- The Headteacher/senior leaders are responsible for ensuring that the Safeguarding Team/ Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher/senior leaders will receive regular monitoring reports from the Safeguarding Team/ Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the Safeguarding Team and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance "Keeping Children Safe in Education" states:
"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"
"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
This review will be carried out by the Governing Body whose members will receive regular information about online safety incidents and monitoring reports if and when they occur. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted Online Safety Lead and reported to the responsible governor - in-line with the DfE Filtering and Monitoring Standards)
- reporting to relevant *governors group/meeting*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL) and Online Safety Lead.

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"
*They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen.

The DSL/Online Safety Lead will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Safeguarding Team.
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- liaise with technical staff
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:

- content
- contact
- conduct
- commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme following Project Evolve.

This will be provided through:

- a discrete programme
- PHSE programmes
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities such as Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level.
- they immediately report any suspected misuse or problem to the Safeguarding Team for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements.
- they supervise and monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's policies, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure

that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

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

"The IT service provider should work with the senior leadership team and DSL to:

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

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and follow it to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority.
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Safeguarding Team for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in school policies

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- seeking their permissions concerning digital images and videos.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in reinforcing the online safety messages provided to learners in school.

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 OSL, 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 in accordance to this poluc. .

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 Subject Lead and Office Staff 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.

SLT 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/AI generators and personal publishing
The school will control access to social networking sites, AI generator sites such as Chat GPT, Gemini and Perplexity 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 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