Lowton West Primary School

Online Safety Policy

Policy reviewed by N. Gould

Date policy reviewed: January 2025

Ratified by Governing Body: January 2025

Dr G. Merrett (Chair of Governors)

Mrs J. Westhead (Headteacher)

Lowton West Primary School Online Safety Policy

Aiming High Together

School Vision

To inspire, achieve and succeed, we will aim high and build dreams and futures together.

Mission Statement

Providing the highest quality education, care and support for the whole school community.

Our mission statement is based on RESPECT:

R *= Recognising the needs of the individual child*

E *= Ensuring a unique and engaging curriculum*

S *= Supporting each other to learn and achieve*

P *= Passionate about providing the highest quality education*

E *= Encouraging creativity, self – expression and imagination*

C *= Creating confident, resilient, life – long learners*

T *= The voice of everybody is heard*

All the above statements help us to understand how we can all make a positive contribution to the school and the wider community.

We will do this through our core values:

- Respect
- Resilience
- Kindness
- Confidence

We also, at Lowton West Primary School, strive to develop and uphold British Values.
The five British values that the Government has identified for schools to focus on are:

- Democracy
- The Rule of Law
- Individual liberty and mutual respect and tolerance of those with different faiths and beliefs
- Developing personal and social responsibility
- Respect for British Institutions

Lowton West Primary School Online Safety Policy

Lowton West Primary School believes that online safety is an essential element of safeguarding children and adults in the digital world.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The Online Safety policy has been revised to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. In adopting this policy, our school community can ensure appropriate procedures are in place to safeguard and promote children's welfare when using online technologies and social media.

The school's Online Safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection, Safeguarding and Child Protection, ICT Security and Social Media Policies and the DfE Keeping Children Safe in Education (KCSIE) 2024. It also considers the DfE guidance Teaching online safety in school (updated January 2023).

End to End online safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband and appropriate filtering through our IT service provided: Benchmark
- National Education Network standards and specifications.
- Appropriate monitoring strategies and systems, including physical monitoring and the monitoring of network activity through the use of Senso software.
-

Writing and reviewing the Online Safety policy

- The school's Online Safety Coordinators are Mrs Gould and Miss Bailey.
- Our Online Safety policy has been written by the school, building on the Wigan Safeguarding Children Board (WSCB) e-Safety strategy and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety policy and its implementation will be reviewed annually.

Teaching and Learning

1. Why Internet use is important

- The Internet and information communication technologies are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

2. Internet use will enhance and extend learning

- Staff will be made aware of and pupils will be educated in the safe use of the Internet.
- Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the Internet and digital communications.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3. Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

1. Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- All users will have their own designated username and password which will be kept secure by themselves.
- Security strategies will be discussed with Wigan LA and the IT service provider.
- All learning platforms accessed via the Internet will have individual usernames and passwords assigned (e.g. SeeSaw, Purple Mash, TT Rockstars and Spelling Shed).

2. E-mail

- Pupils and staff should only use approved e-mail accounts on the school system. This is currently Office 365.
- As part of their Computing curriculum, pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils must immediately tell a teacher if they receive offensive or inappropriate e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, 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.

3. Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

4. Publishing pupil's images and work

- Parents will complete a consent form via the School Spider APP stating what can and cannot be published in relation to their child. These details will be consulted before any work or photographs are published in any context.
- Photographs that include pupils will be selected carefully and where a name is used, only the Christian name will be included.
- Pupils' full names will not be used anywhere on the website.
- Pupil's work can only be published with the permission of the pupil and parents.
- Staff will not keep images of children on personal devices eg. memory sticks, mobile phones or use the images for any other use than in school.
- Staff will not keep images of children on staff i-Pads which leave school premises.
- Staff must ensure that all equipment in school containing images of children, e.g. school lap tops, i-Pads and digital cameras, are locked away securely at the end of the school day and must not be taken out of school.

5. Social networking and personal publishing

- The school will educate people in the safe use of social networking sites and educate pupils on their safe use.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- 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 or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- Parents will receive updates and guidance from school, via emails, school newsletters and the school website in relation to online safety and the use of social media/ APPs/ online gaming etc

6. Managing filtering

- The school will work with Wigan Council and/ or the IT support company, to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator (Mrs Gould) or Headteacher who will report the site to Benchmark (and the local Authority if needed).
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable (using Senso).
- The Online Safety Coordinator (Mrs Gould) will ensure that the filtering system Senso is regularly checked and monitored.

7. Managing videoconferencing / online communication platforms (such as Teams and Zoom)

- IP videoconferencing and online communication platforms (such as Microsoft Teams, Zoom etc) should use the educational broadband network to ensure quality of service and security.
- Pupils will not independently make or answer a videoconference call/ join a Teams or Zoom communication link.
- Calls should only be made or answered in the presence of a supervising adult.
- Audio and video conferencing will be appropriately supervised for the pupils' age.
- Pupils may access Teams online learning provision whilst supervised by teachers. These may be used as part of the school enrichment e.g. a virtual visit from Santa or to support SEND pupils and Year 6 Transition. Teachers will access Teams using Office 365 and their school email address only. No personal emails must be used for school Teams Meetings and school email addresses must not be shared with parents.

8. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Pupils are not allowed to have mobile phones in school except for pupils in Upper Key Stage Two. Upper Key Stage Two pupils are permitted to bring mobile phones to school and are responsible for placing their phones in the designated box on arrival at school. Mobile phones must NOT be kept in pupils' school bags. Mobile phones will be returned to pupils at the end of the school day. Mobile phones must NOT be used at school or on school premises. Pupils should only use their mobile phones once they have stepped off the school premises.

9. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

1. Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource, including any laptop issued for professional use.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stages 1 and 2, access to the internet will be supervised at all times and children will be told which internet site(s) they are allowed to access. Staff will check screens to ensure that the pupils are on the correct website both at the start and during the session.
- Prior to lessons, staff will check websites on the actual systems that are going to be used in school (to ensure that the content is suitable).
- You Tube videos to be watched in class must be checked in school on the day of the lesson, even if they have been checked previously to ensure no inappropriate live adverts or 'pop-ups' appear whilst the video is played. Wherever possible videos will be downloaded and saved prior to the lesson.
- All See Saw learning content will be checked by teachers before uploading to Seesaw to ensure no live news feeds or adverts are present. Website links used by pupils at home should not lead to live Twitter/ Social Media accounts. Parents must be informed of any possible access to live material such as social media links prior to the website being shared with pupils. Parents have been advised of the need to monitor any online learning at home closely.

2. Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Wigan LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit Computing provision to establish if the Online Safety policy is adequate and that its implementation is effective.
- The school will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

3. 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. Any misuse that suggests a member of staff is unsuitable to work with children should be reported to the Local Authority Designated Officer (often referred to as the LADO) in accordance with Wigan Safeguarding Board policies.
- Local Authority Designated Officer (LADO) (wiganlscb.com)
- If the misuse is by the Headteacher it must be referred to the chair of governors in line with Wigan Safeguarding Board Child Protection procedures.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils, parents and staff will be informed of the complaints procedure.

4. Community use of Internet

- The school will liaise with local organisations to establish a common approach to Online Safety.

Communicating Online Safety

1. Introducing the Online Safety policy to pupils

- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and regularly throughout the year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be informed that e-mail accounts provided by the school may be monitored and accessed by the administrator.
- A programme of e-safety training and awareness raising will be put in place in line with the Wigan Safeguarding Children's Board Online Safety strategy.
- The computing Scheme of Work (Purple Mash) includes an online safety unit of work for each year group.
- Pupils and staff must sign an acceptable use agreement before accessing Purple Mash.
- Pupils and staff are given their own Purple Mash username and password to allow them to access Purple Mash both in and out of school.

2. Staff and the Online Safety policy

- All staff will be given the school's Online Safety and Social Media policies and their importance explained.
- Staff will receive regular, up to date and appropriate training regarding online safety, roles and responsibilities and receive guidance on safe appropriate communications.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will be informed that e-mail accounts provided by the school may be monitored and accessed by the administrator.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Staff should understand that phone or on-line communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff working with children using ICT equipment will ensure appropriate risk assessment and supervision is undertaken regarding the safe use of technology, including the safe and responsible use of devices.

3. Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, letters and on the school website.
- From time to time parents and carers may be invited into school for Online Safety awareness sessions to help ensure parents are aware of the most current risks and issues. School will regularly provide updates and online safety information throughout the school year via letters and the school website. Please refer to the Online Safety section of the website for further information.
- If school is informed of any potential risks for pupils relating to Online Safety, for example any safeguarding issues relating to the use of social networking

sites at home, school will ensure parents and carers receive advice and information.

- Parents and carers will be reminded that they must not publish any images or video footage on social network sites before and after each event.

Responding to concerns regarding radicalisation or extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.

When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of Lowton West Primary School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded.

There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Wigan Safeguarding Children Board and/or police.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos. Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time.

Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.

Parent/carers of pupils involved in online bullying will be informed. The Police will be contacted if a criminal offence is suspected.

Other useful Online Safety materials and links:

http://www.thinkuknow.co.uk http://www.ceop.gov.uk
http://www.childnet-int.org/kia/
http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers
http://www.swgfl.org.uk
http://parentinfo.org/

Think then Click

Online-Safety Rules for Key Stage 1

These rules help us to stay safe on the Internet

We ask before we use a tablet, computer or camera.

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do. We tap or click on things we have been shown.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

We tell a grown up if something we see online upsets us.

Think then Click
Online-Safety Rules for Key Stage 2
We ask permission before using the Internet. We ask permission before using any IT equipment in school: tablet, computer or camera. We only use websites that an adult has chosen. We tell an adult if we see anything we are uncomfortable with. We immediately close any webpage we are not sure about. We only e-mail people an adult has approved. We send e-mails that are polite and friendly. We never give out personal information or passwords. We never arrange to meet anyone we don't know. We do not open e-mails sent by anyone we don't know. We do not use Internet chat rooms. We do not share our personal login details with others.