E-Safety Policy
Willow Grove Primary School

‘Be Safe, Be Kind, Be Positive’

Approved by:	Willow Grove Governing Body and Senior Leadership Team	**Date:** September 2025
Created by:	Hazel Smith & Leah Sergeant	
Last reviewed on:	September 2025	
Next review due by:	September 2026	

1. Introduction

Willow Grove Primary School is a specialist Social Emotional Mental Health (SEMH) provider and provides outreach support to mainstream schools in the Wigan Borough. All pupils at Willow Grove have an identified Special Educational Need (SEN), most of our pupils' primary area of need is SEMH. Many of our pupils have experienced early trauma and adversity, and many have attachment difficulties. Willow Grove is committed to providing an educational environment within which our pupils can heal, thrive, learn, and play. All staff work in line with trauma-informed practices, and they have an excellent knowledge of the strategies and resources that are available to meet the needs of pupils with SEMH and additional SEN.

Being safe is one of our core school values and this policy reflects our whole school commitment to safety, in particular online safety.

1.1 Materials on the SWGfl Website have been used to inform this policy. (www.swgfl.org.uk)

1.2 This policy has been developed to ensure that all adults at Willow Grove Primary School are working together to safeguard and promote the welfare of children and young people. This policy has been ratified by the Governing Body and will be reviewed annually.

1.3 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.4 This document aims to put in place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities of using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.5 The Head Teacher or, in their absence, the authorised member of staff for e-safety, School Business Manager has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.6 This policy complements and supports other relevant school and Local Authority policies.

1.7 The purpose of internet use in school is to help raise educational standards, promote pupil achievement and their Digital Literacy, and support the professional work of staff as well as enhance the school's management information and business administration systems.

1.8 The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

1.9 The internet and technologies are ever changing, this policy aims to be as up to date as possible, however this is a quickly evolving technological time.

2. Ethos

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. The Keeping Children Safe in Education 2024 document sets out the legal duties that must be followed to safeguard and promote the welfare of children and young people under the age of 18 in schools and refers to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's Computing facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day. This means that we will intervene in incidents that also occur outside of school if bought to our attention.

2.5 Bullying, harassment, peer on peer or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Code of Conduct Policy.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3. Role and Responsibilities

3.1 The Head Teacher of Willow Grove Primary School will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Member of Staff is assigned as the Digital Lead, they receive appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding, the headteacher.
- All temporary staff and volunteers are made aware of the school's E-Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- The online monitoring system (Senso) is checked regularly and any safeguarding concerns are dealt with in a timely manner.
- Any websites deemed unsuitable for school use will be blocked and reported to the E-Safety lead.

3.2. The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate computing and e-safety training.

3.3 The Designated Members of Staff for E-Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received and signed a copy of the school's Acceptable Use of ICT Policy.
- Ensure that all staff and volunteers are aware of and understand the school's E-Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security, which will be monitored by the IT provider.
- Ensure that the virus protection is regularly reviewed and updated.
- Regularly check files on the school's network and report any concerns to the designated person.

3.4 All staff will:

- Ensure that any incidents of cyber-bullying are reported to the headteacher.
- Will regularly monitor the provisions of online safety in the school.
- Regularly teach online safety lessons within Computing, PSHE and the wider curriculum.
- Comply with acceptable use policy, code of conduct, social media and loan of equipment agreements.

- Ensure that offensive, illegal or radical views, including reference to the “manosphere”, incel culture or misogynist views, that the children may have been exposed to at school or at home are recorded as safeguarding incidents.

4. Teaching and Learning

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and the DfE.

4.3 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.4 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.5 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children.

4.6 Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation and how to keep themselves safe online.

4.7 Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material’s significance.

4.8 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5. Managing Internet Access

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include strict filtering appropriate to the age of the children.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil’s age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable, threatening or of an extremist nature. Pupils will be directed to close screens if needed and report inappropriate content to an appropriate adult. Child- friendly rules linked to the safe use of the internet will be displayed in each classroom and children will be encouraged to know and refer to them when needed (SMART rules).

5.4 If staff or pupils discover unsuitable sites, they should report the URL (address) to the Internet Service Provider via the Computing Co-ordinator/School Business Manager.

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

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

5.7 Pupils will be taught discreet lessons around Cyber Security.

5.8 Pupils will be taught discreet lessons around the use of AI.

5.9 Staff are not allowed to connect to public or unsecure wifi networks.

6. Managing Email

6.1 Personal e-mail or messaging between staff and pupils must not take place.

6.2 Staff may only use approved e-mail accounts on the school system and must inform the Business Manager immediately if they receive an offensive e-mail.

6.3 Pupils must not reveal details of themselves or others in any web space such as an address, telephone number and must not arrange meetings with anyone.

6.4 Access in school to external personal e-mail accounts may be blocked.

6.5 The forwarding of chain letters is not permitted.

6.6 Incoming e-mail should be monitored and attachments by staff members should not be opened unless the author is known.

6.7 Teaching staff will not use their e-mails to contact parents/ carers.

7. Managing Digital Content

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers. Parents/carers will be issued with a consent form for this purpose when their child initially enters school.

7.3 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Head Teacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused.

7.7 Only the first names of pupils will be used on the website, particularly in association with any photographs. Any breach of this will be reported immediately to the DPO.

7.8 Work will only be used on the website with the permission of the pupil and their parents/carers.

7.9 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.10 Staff and pupils will not input school, personal or confidential data into AI platforms.

8. Social Networking and Chat Rooms

8.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

8.2 Pupils will not access any social networking sites whilst at school

8.3 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms, games and apps.

8.4 Pupils will not be allowed to access public or unregulated chat rooms.

8.5 Newsgroups will be blocked unless an educational need can be demonstrated.

8.6 Pupils will be advised to use nick names and avatars when sites as opposed to using their personal information.

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

8.8 Pupils should be advised not to place personal photos on any social network space.

8.9 Pupils should be advised on security and encouraged to set passwords, deny access to unwanted individuals or and instructed how to block unwanted communications.

8.10 Pupils should be encouraged to invite known friends only and deny access to others.

8.11 Pupils and parents should be made aware that some social networks, APPS and games are not appropriate for children of Primary age.

8.12 Staff will not exchange social networking addresses or use social networking sites to communicate with or search for pupils or parents/carers, this includes past pupils.

8.13 Work will be done with all pupils to help them to understand the possible consequences of sharing personal photographs with others and that some photos are permanent. Through this work, they will develop an understanding of their “digital footprint”.

8.14 Pupils and parents must be aware that certain games and apps are not appropriate for the age of primary school children and be advised to adhere to the PEGI rating.

8.15 Personal gaming devices with games that are not age appropriate will not be allowed to be played in school. HR headsets are not permitted in school.

8.16 Any digital content viewed needs to be in line with age restrictions, this includes Netflix, YouTube videos and other streaming services.

9. Mobile Phones

9.1 Phones must be kept in bags or lockers in the staff room at all times and staff should not access their phones during school hours (except lunch times). Staff mobile phones are not permitted in the staffroom. Pupil mobile phones are switched off and kept securely in a box, in a cupboard in class. These are then returned at home time.

9.2 The sending of abusive or inappropriate text messages or files by any means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.

9.3 Staff should disable any notifications sent to their smart watch during school hours.

9.4 Staff are not permitted to have any smart watch with picture taking capabilities.

9.5 Pupils must not connect mobile phones, or gaming devices to the school internet under any circumstances.

9.6 Staff who intend to use personal mobile phones or other mobile technology to access their school email, must ensure that their device is encrypted with a personal password PIN or fingerprint/facial recognition. Passwords and personal information relating to personal devices should be kept confidential.

9.7 Staff should not, under any circumstances take photographs in school using their mobile phone. They must not use their mobile phones on school trips to take photographs of the pupils.

9.8 Mobile phones may be brought to school by pupils and left, turned off, in a secure place within the classroom. The use of mobile phones in any area of school or during lessons is strictly prohibited.

9.9 Pupils will be advised to carefully consider the items they share via mobile phones such as photos and texts. The possible negative impact of "sexting" or sharing personal or explicit photographs with others through apps accessible via mobile phones will be addressed in Jigsaw, PSHE and e-safety lessons.

9.10 Parent/carers and visitors must not take their mobile phones into school, and the devises should be left in the reception area.

9.11 Pupils may not take phones on school trips, including residentials.

9.12 Any inappropriate use of mobile phones, by a pupil or staff, on a school trip can lead to their phone being taken and kept in a secure location. This may lead to disciplinary action.

9.13 Pupils are not allowed on personal devices belonging to staff under any circumstances.

9.14 Staff are permitted to take their mobile phones on trips; the trip lead must take theirs in order to keep in contact with the school. These phones must not be used in front of the children, unless contacting the school, headteacher or SLT, or in case of an emergency.

10. Filtering

10.1 The school will work in partnership with parents/carers; the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 If staff or pupils discover unsuitable sites, URL and content must be reported to the E-Safety lead and appropriate measures will be taken to ensure safety.

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk) by the E-Safety co-ordinator.

10.4 Regular checks by E-Safety and Computing lead will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

10.6 Teaching staff must fully explore new sites before allowing pupils access, monitor pupils closely and make pupils aware of their responsibility in relation to making sensible choices about what they access while online.

10.7 Pupil laptops and iPads are not permitted to access the Staff Wifi, unless authorised by the headteacher for teaching and learning purposes.

11. Internet Access

11.1 All staff must read and sign the school's 'Acceptable Use Policy' before using any school ICT resources.

11.2 Any staff not directly employed by the school, including visitors, volunteers and agency staff will be asked to read this policy before being allowed internet access from the school site.

11.3 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

11.4 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access and whose photographs are not permitted to be taken or shared.

11.5 Staff will supervise access to the internet from the school site for all pupils.

11.6 All pupils will monitor the digital activities of the children when using iPads, laptops or other technology to ensure safe and proper use.

12. Photographic, Video and Audio Technology

12.1 Staff may use school devices to capture school trips and support appropriate curriculum activities. Staff must not use their own devices for this.

12.2 Audio and video files may not be downloaded without the prior permission of the network manager.

12.3 Staff will use the Staff iPad to record and assess pupil attainment and achievement, all staff must ensure they are logged out of any site after use.

12.4 Staff iPad's which have access to email, assessment and the school website must be pin coded. These must be shared with the Digital Lead.

12.5 Images, audio and video taken on iPad devices must be kept secure with the school's network.

12.6 Images of past pupils will be deleted in accordance with GDPR regulations.

13. Assessing Risks

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies can bypass school filtering systems.

13.2 Due to international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly. The headteacher will access and inform the relevant authorise if necessary.

13.5 The Head Teacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

13.6 Access to any websites involving gambling, radicalisation, explicit materials, illegal material, chat rooms or financial scams is strictly forbidden and will be dealt with accordingly.

13.7 If a child protection incident is suspected, the school's child protection procedure will be followed, the headteacher will be informed and the police contacted.

13.8 A designated person will complete an annual e-safety review to ensure that appropriate measures are in place.

14. Pupils

14.1 Responsible Internet use, covering both school and home use, will be included in the PSHE and Computing online Safety curriculum.

14.2 E-safety will be a key part of a progressive curriculum that is flexible, relevant and engages pupils' interest. The Computing curriculum will be used to promote e-safety and Digital literacy through teaching pupils how to protect themselves from harm and how to take responsibility for their own and others safety.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

14.4 Pupils will be made aware that internet use will be closely monitored and that misuse will be dealt with appropriately.

14.5 Pupils may be temporarily banned from using the computers or iPads if repeated offenses occur.

14.6 Pupils are not allowed to bring in VR headsets as their content cannot be monitored by staff.

14.7 Pupils are not allowed on their personal technology devices within school time.

15. Staff

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's 'Acceptable Use Policy' and will be provided with a copy of the Acceptable Use Policy and its importance explained. Staff will be required to resign the document if any amendments have been made.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

15.2 Staff are not permitted to link devises to parent/carer home Wifi when conducting offsite visits. They can hotspot from an approved work device.

16. Maintaining Security

16.1 Personal data sent over the network will be encrypted or otherwise secured.

16.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

16.3 USB drive must not be used under any circumstances, including those used by outside agencies on school technology.

16.4 The Digital Lead, Business Manager, Receptionist and Headteacher are to receive enhanced annual cyber security training.

16.5 All staff to receive cyber security training annually.

16.6 A Cyber security response plan is agreed with the IT provider and shared with staff. If a security breech occurs, this plan will be followed, and the relevant people will be noticed.

MAINTAINING SECURITY FOR REMOTE WORKING

16.5 All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 12 characters, with a combination of upper and lower-case letters, numbers and special characters.
- Multi-factor authentication used for Microsoft 365 logins when off site. Microsoft authenticator app to be used.
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Making sure staff lock their device when leaving it unattended.
- Not sharing the device among family or friends.
- Installing antivirus and anti-spyware software and keeping operating systems up to date – always install the latest updates

17. Dealing with Complaints

17.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures. Staff may record incidents using the school Behaviour Watch system.

17.2 The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Head Teacher immediately.

17.3 Pupils and parents/carers will be informed of the complaints procedure.

17.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.5 There may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files, held on the system
- Referral to the police.

18. Parent/ Carer Support

18.1 Parents/carers will be informed of the school's Internet Policy which may be accessed on the school website.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.

18.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.

18.4 Parent/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP) and the NSPCC site. Parents can access safer internet resources on the Online Safety Information for Parents section on the school website.

18.4 Dojo will be used to sharing photos and information with parents/ carers. See the Dojo policy for more information regarding acceptable use of Dojo.

19. Safeguarding and Remote Learning

19.1 With the increased use of digital technologies that comes with remote learning, safeguarding implications need careful consideration.

19.2 Parents/carers are advised to spend time speaking with their child(ren) about online safety and reminding them of the importance of reporting to an adult anything that makes them feel uncomfortable online.

19.3 Online safety concerns should still be reported to the child's class teacher and school's Online Safety Lead as normal. Parents can do this by phoning the school office.

19.4 The following websites offer useful support:
•Childline - for support
•UK Safer Internet Centre - to report and remove harmful online content
•CEOP - for advice on making a report about online abuse
In addition, the following sites are an excellent source of advice and information:
•Internet matters - for support for parents and carers to keep their children safe online
•Net-aware - for support for parents and careers from the NSPCC
•Parent info - for support for parents and carers to keep their children safe online
•Thinkuknow - for advice from the National Crime Agency to stay safe online

19.5 If parents have any online safety concerns that need discussing, they can contact us through the usual channels and one of our Safeguarding Leads will get in touch.

19.6 Staff should continue to be vigilant and follow our usual online safety and safeguarding / child protection policies and procedures, contacting a safeguarding lead directly by phone in the first instance.

20. Links with Other Policies and Documents

This policy links to the following documents:

- Keeping Children Safe in Education
- Safeguarding and Child Protection Policy
- Acceptable Use of Technology Policy
- Loan of Equipment Agreement
- Anti Bullying Policy
- Staff Code of Conduct Policy
- Cyber Security Response Plan
- Class DoJo policy

Next review due by:	Autumn Term 2026