LONGWILL SCHOOL FOR DEAF CHILDREN

(Please read in conjunction with the Computing Policy, Safeguarding Policy, Behaviour Policy, Remote and Blending Learning, Information Security Policy, Acceptable Use Policy (AUP) and Complaints Policy)

E-safety Policy

September 2025

Staff covered by this procedure:	All Staff
Approved By:	Longwill Governing Body
Date:	September 2025
Next Review Date:	36 months from last approval

Signed  Date 25.09.25

(Chair of Governors)

Signed  Date 25/09/25

(Headteacher)

Rationale for E-Safety Policy and Longwill School

At Longwill School, we recognise the educational value of using the internet and digital technologies across the curriculum. To ensure pupils can engage safely and confidently online, we have developed a robust E-Safety Policy that outlines clear expectations for both pupils and staff.

The policy covers not only internet use but also a wide range of digital platforms and communication tools—including Microsoft Teams, mobile devices, iPads, and emerging technologies. It highlights both the benefits and potential risks, offering practical guidance for safe and responsible use.

Our E-Safety Policy and curriculum are fully aligned with *Keeping Children Safe in Education (KCSIE 2025)*. Staff are expected to help protect pupils from online harassment, bullying, and coercion, and to uphold the principles of the four C's:

- **Content** – Preventing access to harmful or inappropriate material
- **Contact** – Recognising and responding to unsafe online interactions
- **Conduct** – Promoting respectful behaviour and digital responsibility
- **Commerce** – Raising awareness of scams, phishing, and financial risks

In line with our Computing Policy, we also aim to ensure pupils are digitally literate and understand how to behave safely and respectfully online.

This policy supports our wider safeguarding responsibilities (see our Safeguarding Policy) and reflects our commitment as a UNICEF Rights Respecting School. It upholds Articles 17, 19, 31, and 36 of the UN Convention on the Rights of the Child, which affirm every child's right to access safe information, protection from harm, and enriching experiences both online and offline.

Core Principles of Internet Safety

Digital literacy is essential for all pupils, but unregulated internet access carries risks, including exposure to harmful content. Longwill School's E-Safety Policy is built on five core principles to ensure safe, purposeful use of technology:

1.Guided Educational Use:
Internet use must be purposeful, task-focused and closely supervised to maximise learning and minimise risk.

2. Risk Awareness and Response
Pupils are taught to recognise online dangers such as grooming, extremism and cyberbullying. Staff regularly assess risks and ensure pupils know how to respond and report concerns.

3. Shared Responsibility

Online safety is a collective effort involving staff, governors, parents and pupils. We balance education with technical safeguards to promote responsible use.

4. Continuous Monitoring
Technology evolves rapidly. We monitor usage through secure systems, including firewalls and Securus software, and prohibit high-risk platforms like unmoderated chat rooms. Clear rules are displayed to guide safe choices.

5. Tailored Strategies
We implement age-appropriate strategies to limit exposure to harmful content, promote digital responsibility, and support safe online learning. These are reviewed regularly for effectiveness.

Integration with School Policies
Our E-Safety Policy is closely aligned with key school policies; including Computing, Safeguarding, Behaviour, Acceptable Use (AUP), and Information Security, for both pupils and adults.

This ensures online safety is embedded across all areas of school life and supports our wider safeguarding commitments.
You can find all related policies at: www.longwill.bham.sch.uk/policies

Importance of the Internet and Digital Communications

Digital technology plays a significant role in modern education, communication, and daily life. According to **Ofcom's Technology Tracker 2025**, 97.8% of homes in the UK now have access to the internet. At Longwill school, is embedded within the statutory curriculum and serves as a vital tool for learning for both pupils and staff.

Importance of E-safety for D/deaf children
Deaf children due to their age, social understanding and disability are more susceptible to cyberbullying, scams and grooming online (E-safety Commissioner 2020; Bryce & Glasby 2020). In fact, some research indicates that deaf children are three times more likely to experience abuse online (Glickman 2013).

Parents and E-safety for D/deaf children
Recent research by Longwill's Computing Lead (Hall, 2023) found that many parents feel less confident in protecting their D/deaf children online compared to hearing children or themselves. In response, Longwill offer dedicated workshops for parents and carers, providing practical advice and support to help safeguard their children online.

Enhancing Learning through the Internet

- **Safe and Filtered Access:** School internet access is designed specifically for teaching and learning and includes age-appropriate filtering systems.
- **Defined Boundaries for Use:** Pupils and staff follow clearly defined rules for safe digital engagement. Pupils must agree to a child-friendly Acceptable Use Policy (AUP) each time they log in.
- **Skill Development:** Pupils are taught how to conduct safe and effective research online, including how to retrieve and evaluate information and understand ethical issues such as copyright law**.**.

The National Curriculum

The computing curriculum aims to ensure pupils are "responsible, competent, confident and creative users of information and communication technology". (National Curriculum 2013)

In Key Stage One the pupils will be taught to:

- use technology respectfully and with purpose to create, organise, store, edit and retrieve digital content confidently
- understand the importance of keeping personal information private and know how to seek help if they feel unsure or concerned about anything they encounter online.

In Key Stage Two the pupils will be taught to:

- understand how the internet offers a range of services, including the world wide web, and explore its potential for communication and collaboration
- use search technologies effectively, recognise how results are selected and ranked, and critically evaluate digital content
- use technology safely, respectfully and responsibly; identify acceptable and unacceptable behaviour; and know how to report concerns about online content or contact.

Staff Responsibilities:

Vigilance: Be alert to signs of harm, distress linked to online safety concerns and report them immediately to the DSL.

Confidentiality: Share safeguarding digital concerns through formal channels and with appropriate staff.

Professional Conduct: Model respectful, safe behaviour at all times, including online, during digital communication whether at school or off-site.

Training and Compliance: Complete all safeguarding and e-safety training, and follow school policies consistently, including those on acceptable use and mobile technology.

Supportive Practice: Create safe spaces for pupils to share online concerns, listen without judgment, and act in their best interests.

Digital Awareness: Be familiar with the school's filtering and monitoring systems, understand your role in promoting safe digital use, and respond appropriately to any alerts or incidents and relay them to the DSL.

E-safety Curriculum

In addition to the computing curriculum, a revised E-safety curriculum is being taught at Longwill to ensure the children are confident with the four Cs included in the KCSIE 2025 guidance. This includes expected *Conduct* whilst online. Who they should or should not talk to when online (Contact). What is appropriate content and what to do if they come across inappropriate *content.* This includes learning how to critically analyse content for credibility. Finally, *commerce* (how to deal with online advertising and how to protect themselves from scams.

Critical Evaluation of Online Content

Pupils must learn to critically evaluate the information they encounter online. Older pupils are trained to validate the accuracy of materials and respect intellectual property. This training is essential for helping pupils become discerning consumers and creators of digital content (Zlatkin-Troitschanskaia,et al. 2022).

Cyber Bullying

Child-on-child cyberbullying has risen in recent years along with the increased use of smartphones and social networks (Bokolo and Liu 2023). Through the E-safety curriculum children will be taught the skills for correct digital etiquette such as being polite when communicating online (Kammer and Hays 2023) and what to do if someone is unkind, sends or requests inappropriate content.

During E-safety lesson and Relationship, Personal Social Health and Education (RPSHE) children are reminded what to do if they access inappropriate content (switch the screen off and tell an adult).

Managing Internet Access

Information System Security

School ICT systems are regularly reviewed for security, with up-to-date virus protection and encryption for personal data transfers. Strict controls are in place for unapproved software and media, and wireless access points are secured with WPA2 encryption.

Email Usage

- **Supervised Access:** Pupils are only allowed access to the internet under direct adult supervision.

Publishing Content and Managing Social Media

- **No Personal Information:** Personal contact information for staff or pupils is never published online.
- **Controlled Image Usage:** Photos or videos of pupils are carefully selected, and pupils' full names are never used in conjunction with images.

Social Networking

Access to social networking sites is blocked unless explicitly approved for educational purposes. Pupils are advised on the importance of online privacy and security, particularly the risks of sharing personal information.

Filtering and Monitoring

We work closely with our internet service providers to regularly review and improve systems that protect pupils online. Longwill School uses Securus software to monitor internet activity and ensure compliance with E-safety guidelines. The Headteacher oversees the strategic implementation of filtering and monitoring, while the Designated Safeguarding Lead (DSL) ensures alerts are reviewed and acted upon appropriately. Technical staff are responsible for maintaining the systems and reporting any concerns to the DSL.

Technologies in Use

Staff are trained to manage the challenges posed by devices such as iPads and mobile phones, which can bypass school filtering systems. Clear policies ensure safe use within school.

All remote video calls must use school Teams accounts. Personal phones may be used to contact parents if the number is withheld.
See the Remote and Blended Learning Policy for full guidance.

Policy Decisions and Risk Management

All staff and pupils are required to read, understand and sign the school's Acceptable Use Policy (AUP), which is reviewed regularly to reflect evolving risks and technological advancements. The school takes all reasonable

precautions to prevent access to inappropriate content, but it also acknowledges that it cannot guarantee total protection.

Handling E-Safety Complaints and Incidents

Complaints related to internet misuse are managed by senior staff in line with school's Complaints Policy. Safeguarding concerns, including cyberbullying, are addressed in line with our Safeguarding, Behaviour, and Complaints Policies; all available at (https://www.longwill.bham.sch.uk/policies).

Conclusion

The Longwill School E-Safety Policy is designed to provide a secure and enriching digital environment for all pupils and staff. It reflects our commitment to safeguarding, pupils' rights, and educational excellence in the digital age. The policy is reviewed regularly to stay responsive to emerging risks and technologies.

Gemma Hall
Computing Lead
October 2024

Updated 25/09/25 Alison Jackson

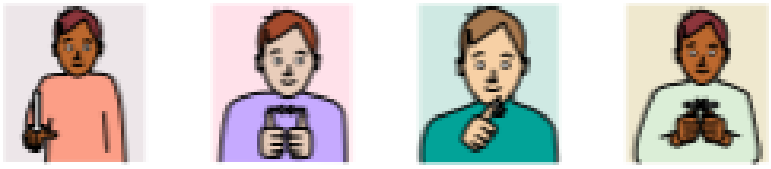
Unicef Rights of the Child:
Article 17
You have the right to get information that is important to you and will not damage your well-being.

Pupil Acceptable Use Agreement

This is how we stay safe when we use computers:

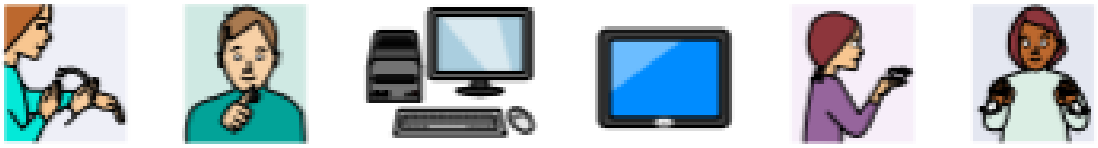
- I will ask a teacher if I want to use the computers/tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher if I see something that upsets me on the screen and tell a member of staff
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):



Pupil Acceptable Use Agreement

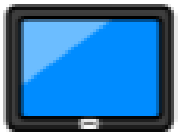
Using computers safely



I will ask a teacher if I want to use the computers/tablets.

I will only use activities that a teacher has told or allowed me to use.





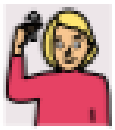

I will take care of computers/tablets and other equipment.


I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong.









I will tell a teacher if I see something that upsets me






I know if I break the rules I might not be allowed to use a computer/tablet

Longwill School
Bell Hill
Northfield
Birmingham

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of computing skills, Longwill School is providing supervised access to the internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Birmingham City Council operates a filtering system that restricts access to inappropriate materials.

This may not be the case at home and we can provide references to information on safe internet access if you wish. We also have leaflets from national bodies that explain the issues further.

Whilst we try to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the internet. The School will not be liable for any damages arising from your child's use of the internet facilities.

Should you wish to discuss any aspect of internet use please contact school to arrange an appointment.

Yours sincerely

Mrs Alison Carter
Headteacher

References

Bokolo, G and Liu, Q. 2023. Combating Cyberbullying in Various Digital Media Using Machine in Lahter, M., Pathan, A, K., Maleh, Y. Combatting Cyberbullying in Digital Media with Artificial Intelligence. Talor and Francis. Oxon.

Bryce, I. and Glasby, K. 2020. Child Sexual Abuse in the context of Disability in Bryce, I.B. and Petherick, W. ed(s) *Child Sexual Abuse Forensic Issues in Evidence, Impact and Management*. [Online] London: Academic Press. [Date accessed 21 July 2023] Available from: https://www.google.co.uk/books/edition/Child_Sexual_Abuse/3HfLDwAAQBAJ?hl=en&gbpv=1&printsec=.

E-safety Commissioner. 2020. *Online safety for young people with intellectual disability*. [Accessed 3 August 2023] Available from https://www.esafety.gov.au/sites/default/files/2020-12/Online%20safety%20for%20young%20people%20with%20intellectual%20disability%20report.pdf.

Glickman, N. and Pollard, R.Q. 2013. Deaf Mental Health Research in Glickamn, N.S. ed(s) *Deaf Mental Health care*. New York: Routledge.

Hall, G. 2023. Online Safety for deaf children, a parent's perspective. Leeds University

IICSA (Independent Inquiry Child Sexual Abuse). 2022. *Child Sexual exploitation by organised networks – investigations report: February 2022*. Accessed [10 July 2023] Available from: https://www.iicsa.org.uk/document/child-sexual-exploitation-organised-networks-investigation-report-february-2022.html.

Kammer, J and Hays, L. 2023. Digital Literacy Made Simple: Strategies for Building Skills. Strategies for Building Skills Across the Curriculum. Internation Society for Technology in Education.

KCSIE, 2024. Keeping Children Safe in Education. Available from: *https://assets.publishing.service.gov.uk/media/66d7301b9084b18b95709f75/Keeping_children_safe_in_education_2024.pdf.*

ONS (Office of National Statistics). 2021. *Prevalence of gearing impairments in the UK* [Accessed 22 July 2023] Available from: https://www.ons.gov.uk/aboutus/transparencyandgovernance/freedomofinformationfoi/prevalenceofhearingimpairmentsintheuk

Zlatkin-Troitschanskaia, O., Alexander, P and Pellegrino, J. 2022. Assessing Information Processing and Online Reasoning as Prerequisite for Learning in Higher Education. Frontiers in Education. SA.

Winarsih, M. Wahyuni, L and Manik, U. 2020. Reproductive Health Animations as Efforts to Prevent Sexual Harassment in Deaf Students. In Indonesian of Educational Journal Vol 9 No 3.

RISK ASSESSMENT for E-SAFETY LONGWILL SCHOOL FOR THE DEAF

HAZARDS IDENTIFIED (Task/Activity/Situation/Process /Stressor)	Persons at Risk	RISKS IDENTIFIED	Initial Risk Rating	Existing Controls	Interim Risk Rating	Further Measures to be taken	Residual Risk Rating	Comments
Using the internet in school Risk of exposure to inappropriate material in terms of **Content**	Pupils & Adult users	Risks from: Racist, Hate, Violent Exploitative Bullying websites Blogs (www.youtube.com) Extremist or Radicalised		BGFL Filters PCE v6 E-Safety Policy and Guidelines Twilight inset Planned intent usage No surfing Explicit teaching of 'internet wise' skills Internet safety rules Acceptable Use Policy	LOW			
Using the internet in school Risk of exposure to inappropriate material in terms of **Contact**	Pupils & Adult users	Risks from: Bullying emails or texts Grooming Blogs Radicalisation Extremism		BGfL filters PCE v6 Anti Bullying Policy Behaviour Policy RPSHE policy Internet safety rules E-Safety Policy No chatroom access Child-friendly search-engines (e.g. Kiddle)	LOW			
Using the internet in school Risk of exposure to inappropriate material in terms of **Commerce**	Pupils	Risks from: Advertising Pupil inability to discern truth from advertising		BGfL filters PCE v6 RPSHE Internet safety rules	LOW			
Using the internet in school Risk of exposure to inappropriate material in terms of Conduct	Pupils & Adult users	Risks from: Bullying emails or texts Grooming Blogs Radicalisation Extremism		BGfL filters Anti Bullying Policy Behaviour Policy RPSHE policy Internet safety rules E-Safety Policy No chatroom access Internet Safety Week	LOW			
Using email in school	Pupils & Adult users	Risk of inappropriate **email** content/usage		BGfL Filters Teach children to report issues Email unit at KS2 E-Safety Policy	LOW	Replace usernames with numbers		
School website	Pupils	Risk of identifying pupils		Pupils will not be named. Parents agreement sought No names, addresses used	LOW			

Name of Assessor(s) Alison Carter Signatures(s) _____ Date of Assessment: October 2024

Name of Manager: _____ Signatures(s) _____ Date for Review: October 2027