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

October 2024

Staff covered by this procedure:	All Staff
Approved By:	Longwill Governing Body
Date:	September 2024
Next Review Date:	36 months from last approval

Signed ………………………………… Date ……………………………

(Chair of Governors)

Signed ………………………………… Date ……………………………

(Headteacher)

Rationale for E-Safety Policy at and Longwill School

Longwill School firmly believes in the educational advantages of utilising the internet as part of the curriculum. Recognising the risks associated with inappropriate usage, the school has developed a comprehensive approach to ensure pupils can engage safely and effectively online.

The E-Safety Policy covers the safe use of the Internet but also a broad range of electronic communications technologies, including Microsoft Teams, mobile devices, iPads, and other emerging technologies. By highlighting the benefits and potential dangers of these tools. The policy ensures that pupils and staff have clear guidance on safe and responsible usage.

The E-safety policy and Curriculum at Longwill has been updated in line with Keeping Children Safe in Education guidance (KCSIE 2024). Including the expectation that schools protect pupils from harassment, bullying and being coerced online whilst at school (paragraph 137 Page 39). The policy also continues to encompass the four C's (paragraph 135 page 38). Ensuring the pupils are protected from accessing harmful ***c**ontent*, they are aware of the dangers regarding ***c**ontact* with individuals online and what to do in these situations. What risks are involved with ***c**ommerce* including scams and how to protect themselves. Finally, in accordance with the Computing Policy, ensure the pupils are digitally literate and are aware of how they should ***c**onduct* themselves (and how others should behave) whilst online.

The policy also aligns with our safeguarding commitments (please see the Safeguarding Policy https://www.longwill.bham.sch.uk/policies). In addition, Longwill is a UNICEF Rights Respecting school, the commitment to keep pupils safe online links with Articles 17, 19, 31, and 36 of the Convention on the Rights of the Child, which emphasises children's rights to information, protection, and safe, enriching experiences both on and offline.

Core Principles of Internet Safety

The widespread integration of the internet into daily life makes digital literacy a critical skill for all pupils. However, unregulated access to the internet poses risks, including exposure to inappropriate or dangerous content. Our E-Safety Policy is grounded in the following five core principles:

1. **Guided Educational Use:** The internet is an invaluable educational resource, allowing pupils to access information globally and communicate easily with others. However, internet usage within the curriculum must be purpose-driven, task-oriented, and closely supervised to maximise educational value while mitigating risks.

2. **Risk Assessment:** The digital world presents dangers such as grooming, extremism, and cyberbullying. Pupils must be equipped with the knowledge and skills to recognise and navigate these threats. This

includes performing regular risk assessments and ensuring pupils know how to respond to inappropriate content and who to report it to.

3. **Shared Responsibility:** Internet safety is a collective effort, involving staff, governors, parents, and pupils. A balance between educating pupils to use the internet responsibly and regulating access through technical solutions is crucial.

4. **Ongoing Review and Monitoring:** The rapidly evolving nature of digital technology necessitates continuous monitoring to ensure safe usage. For example, chat rooms are banned in our school. Clear, prominently displayed rules help guide pupils toward responsible decision-making. The school has online monitoring systems and firewalls to protect users.

5. **Appropriate Strategies:** To promote safe online behaviour, we implement a range of strategies tailored to our school's specific needs. These strategies focus on limiting access to inappropriate content, fostering responsibility, and guiding pupils toward educational activities. The effectiveness of these measures is monitored and reviewed regularly.

Integration with School Policies

The E-Safety Policy is linked with other key school policies, including those for Computing, Safeguarding, Behaviour, Acceptable Use (AUP) and Information Security Policies for both adults and pupils (These can be found at: https://www.longwill.bham.sch.uk/policies. This comprehensive approach ensures that E-safety is a central component of school life, integrated with broader safeguarding efforts.

Teaching and Learning Objectives

Importance of the Internet and Digital Communications

Digital technology plays a significant role in modern education, business, and personal interactions. According to the UK Census 2020, 96% of homes in the UK now have access to the internet (ONS 2021). Recognising this, internet usage in 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 (IICSA 2022; Winarsih 2020; Glickman 2013).

Parents and E-safety for D/deaf children

The Computing Lead at Longwill recently submitted Master level dissertation regarding E-safety for D/deaf children from the perspective of parents. The primary research from this indicated that parents in general feel less confident in keeping their D/deaf children safe online than themselves or other hearing children (Hall 2023).

In response to this, Longwill will offer parent and carer workshops in relation to E-safety and give support and advice on how to try and help protect their child online and why this is needed.

Enhancing Learning through the Internet

- **Safe and Filtered Access:** School internet access is designed specifically for teaching and learning and includes age-appropriate filtering.
- **Defined Boundaries for Use:** Boundaries around appropriate use are clearly communicated to pupils and staff, ensuring safe engagement with digital technologies. Pupils must agree to a child-friendly Acceptable Use Policy (AUP) each time they log into the school system.
- **Skill Development:** Pupils are taught how to conduct safe and effective research online, including critical skills like knowledge retrieval, evaluation, and ethical considerations 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 purposefully to create, organise, store, manipulate and retrieve digital content.
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In Key Stage Two the pupils will be taught to:

- understand how the internet provides multiple services, such as the world wide web; and the opportunities for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

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 2024 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, in particular, 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 continually review and improve systems designed to protect pupils. Longwill School uses SECURUSsoftware to monitor internet activity and ensure compliance with E-safety guidelines.

Technologies in Use

We recognise the challenges posed by devices such as iPads and mobile phones, which can bypass school filtering systems. Staff receive training on how to manage these technologies effectively, and strict policies are in place to ensure they are used safely within the educational context.

In the case of remote learning, all video calls between staff, pupils and parents are made via the schools Teams accounts. Personal devices can be used to call parents provided the number is withheld (See Remote and Blending Learning Policy available from: https://www.longwill.bham.sch.uk/policies)

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 regarding internet misuse are handled by senior staff in line with the Complaints Policy. Further to this, issues involving safeguarding including cyberbullying are managed in line with the school's Safeguarding, Behaviour and Complaints Policies. These policies can be accessed via the school website (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, student rights, and educational excellence in the digital age. The policy is regularly reviewed to remain responsive to new challenges and opportunities presented by evolving technology.

Gemma Hall
Computing Lead
October 2024

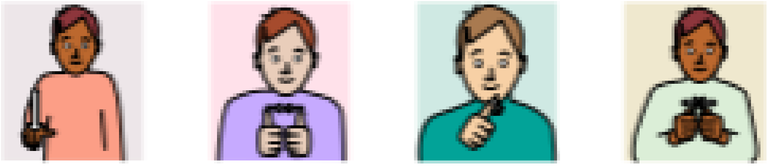
Unicef Rights of the Child:
Article 17
You have the right to get information that is important to you and will not damage your well-being.

Pupil Acceptable Use Agreement

<u>This is how we stay safe when we use computers:</u>

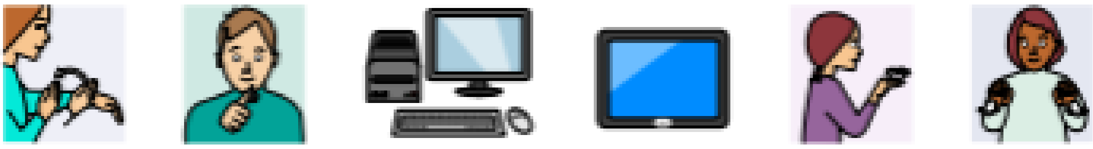
- I will ask a teacher if I want to use the computers/tablets
- I will only use activities that a teacher has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher if I am not sure what to do or if I think I have done something wrong
- 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):



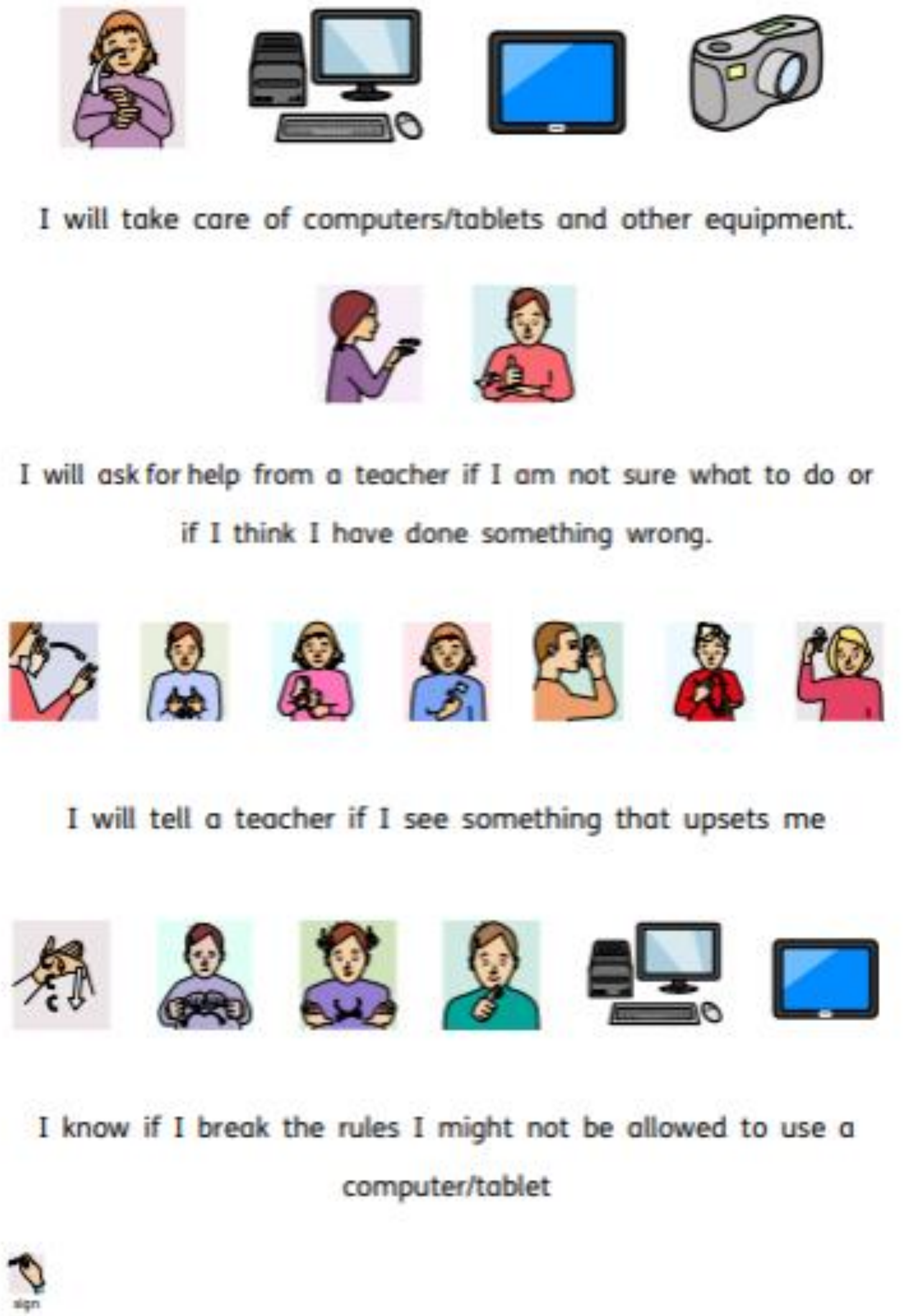
Pupil Acceptable Use Agreement

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 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 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 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