

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

June 2026

Staff covered by this procedure:	All Staff
Approved By:	Longwill Governing Body
Date:	June 2026
Next Review Date:	12 months (or sooner if legislation changes prior to this.

Signed ... 

Date June: 2026

(Chair of Governors)

Signed ...  ...

Date June 2026

(Headteacher)

L School E-Safety Policy

Policy Statement

Longwill School is committed to providing a safe, supportive and inclusive learning environment where all pupils can use digital technologies safely, responsibly and effectively. As a primary school for deaf children, we recognise that our pupils may face additional barriers when accessing information and communicating online. We therefore place a strong emphasis on teaching online safety skills and safeguarding children from potential harm.

Longwill School is proud to hold the Gold Award for the United Nations Convention on the Rights of the Child (UNCRC). This policy reflects our commitment to promoting children's rights, particularly:

- Article 3 – The best interests of the child.
- Article 13 – Freedom of expression.
- Article 16 – Right to privacy.
- Article 17 – Access to reliable information.
- Article 19 – Protection from abuse and neglect.
- Article 36 – Protection from exploitation.

The school believes that all children have the right to access technology safely and to be protected from online risks. In addition Longwill School operates a strict GDPR-compliant approach to all aspects of information management. The protection of children's personal data is considered a fundamental safeguarding responsibility and forms part of the school's commitment as a Gold Rights Respecting School under the UNCRC.

Aims

This policy aims to:

- Protect pupils and staff from online risks and harm.
- Promote safe, responsible and respectful use of technology.
- Support pupils in developing digital resilience and critical thinking skills.
- Ensure compliance with safeguarding and data protection requirements.
- Provide clear expectations for staff, pupils, visitors and volunteers.

Why Online Safety is Important for Deaf Children

Research shows that deaf children and young people can be at increased risk of abuse, exploitation and online scams.

Studies have found that disabled children are approximately three to four times more likely to experience abuse than their non-disabled peers. Communication barriers, social isolation, and difficulties accessing information can increase vulnerability.

Research from the National Deaf Children's Society (NDCS) has highlighted that deaf children may:

- Be more vulnerable to online grooming and exploitation.
- Find it more difficult to identify online risks due to language and communication barriers.
- Experience higher levels of social isolation, making them more susceptible to manipulation online.
- Be at greater risk of cyberbullying.

- Be more likely to trust information shared through social media without recognising fraudulent or misleading content.

For these reasons, Longwill School places a strong emphasis on teaching pupils how to identify scams, misleading information, unsafe online relationships and inappropriate online behaviour.

Curriculum and Online Safety Education

Longwill School follows the Evolve 360 Online Safety Framework. Online safety is taught throughout the year and is embedded within the wider curriculum and safeguarding provision.

The following objectives are taught:

Autumn A: Managing Online Information and Self-Image and Identity

- Includes work linked to Anti-Bullying Week.
- Focus on recognising trustworthy information, online influences and positive digital identities.

Autumn B: Online Bullying

- Understanding cyberbullying.
- How to seek help and support.
- Respectful online behaviour.

Spring A: Privacy and Security

- Linked to Safer Internet Day.
- Passwords, personal information, scams and online security.

Spring B: Copyright and Ownership

- Understanding ownership of digital content.
- Respecting the work of others.
- Safe use of images and media.

Summer A: Health, Wellbeing and Lifestyle

- Linked to Screen-Free Week.
- Healthy screen habits.
- Managing online and offline balance.

Summer B: Online Relationships and Online Reputation

- Safe online communication.
- Understanding digital footprints.
- Positive online relationships.

The Computing Lead will deliver a whole-school assembly linked to each Evolve 360 objective. Class staff will reinforce these messages regularly through classroom discussion, PSHE lessons, safeguarding activities and day-to-day interactions with pupils.

National Developments: UK Social Media Restrictions for Children

In June 2026, the UK Government announced landmark measures to improve children's online safety. On 15 June 2026, the Prime Minister confirmed plans to introduce a ban on social media platforms providing services to children under the age of 16. The proposed legislation is expected to be implemented from 2027 following consultation and regulatory preparation by Ofcom.

The proposals are intended to reduce children's exposure to:

- Online grooming and exploitation.
- Cyberbullying.
- Harmful and inappropriate content.
- Online scams and fraud.
- Addictive platform features designed to maximise screen time.
- Contact from unknown adults online.

The government has also announced restrictions on features such as livestreaming and communication with strangers for children and young people, alongside stronger age-verification requirements for technology companies.

As a school for deaf children, Longwill School recognises that many pupils may require additional support to understand online risks and to access online safety information. The school will continue to work closely with families to promote safe and age-appropriate use of technology, while supporting pupils to develop the knowledge and skills needed to navigate the online world safely and responsibly.

Longwill School supports the principles behind these national safeguarding measures and will continue to educate pupils about the safe use of social media, online communication, digital wellbeing and the importance of seeking help if they encounter anything online that makes them feel worried, unsafe or uncomfortable. This work will be delivered through the Evolve 360 Online Safety Curriculum, whole-school assemblies, classroom discussions and engagement with parents and carers.

Roles and Responsibilities

The **Governing Body** will:

- Ensure appropriate online safety policies and procedures are in place.
- Monitor safeguarding arrangements relating to technology.
- Support the school in maintaining effective filtering and monitoring systems.

The **Headteacher** will:

- Ensure this policy is implemented consistently.
- Promote a strong culture of safeguarding and online safety.
- Ensure staff receive appropriate training.

The **Designated Safeguard Lead (DSL)** will:

- Manage online safety concerns and incidents.
- Liaise with external agencies where necessary.
- Support staff and families with safeguarding concerns linked to technology.

The **Computing Lead** will:

- Coordinate the Evolve 360 curriculum.

- Coordinate the Computing curriculum.
- Deliver whole-school assemblies.
- Monitor online safety provision.
- Support staff with online safety teaching.

All staff must:

- Model safe and professional online behaviour.
- Report concerns immediately.
- Follow the school's Acceptable Use Policy.
- Teach and reinforce online safety messages regularly.

Acceptable Use

All users of school technology are required to sign an Acceptable Use Agreement before accessing school devices, systems or networks (these can be found in the appendix).

This includes:

- Pupils
- Staff.
- Governors.
- Volunteers.
- Contractors with network access.

Users are expected to:

- Use technology safely and responsibly.
- Protect passwords and personal information.
- Report concerns immediately.
- Follow safeguarding and data protection procedures.

Failure to comply may result in disciplinary action and/or removal of access rights.

Mobile Phones and Personal Devices

To safeguard pupils and maintain a secure environment:

Staff Mobile Phones

- Personal mobile phones must not be used in areas where children are present except in emergencies or where specified authorised.
- Phones should remain stored securely in lockers during teaching sessions.

Pupil Mobile Phones

- Any pupil bringing a phone into school must hand these into the school office upon arrival at school
- Phones must not be used during lessons, breaks or other school activities.

Visitors

All visitors will be informed that:

- Mobile phones should not be used in areas where children are present.
- Photography and video recording are prohibited unless expressly authorised by the Headteacher.
- Visitors must always comply with safeguarding requirements.
- Parents, carers and visitors will be reminded that any photographs or video recordings taken during school performances are for personal use only. Images or footage that include other pupils must not be shared on social media, messaging platforms or other public forums, as consent may not have been obtained from all families. The school requests that all visitors respect the privacy, safety and data protection rights of every child.

Smart Watches and Wearable Technology

In line with safeguarding expectations and current Ofsted guidance regarding professional boundaries and internet-connected devices:

- Staff may wear smart watches in school provided that Bluetooth and other connectivity features are switched off. Smart watches must not be used for messaging, internet access, photography, audio recording or communication whilst working with pupils.
- Any wearable technology used in school must not compromise safeguarding, confidentiality or professional conduct.
- Staff should seek guidance from senior leaders if unsure whether a device is appropriate.

Filtering and Monitoring

The school operates filtering and monitoring systems (name) to:

- Protect pupils from harmful content.
- Prevent access to inappropriate websites.
- Monitor safeguarding concerns.
- Support compliance with Keeping Children Safe in Education (KCSIE).

Any concerns identified through monitoring will be addressed in line with safeguarding procedures.

Reporting Concerns

All members of the school community should report concerns immediately.

Examples include:

- Cyberbullying.
- Inappropriate content.
- Online grooming concerns.
- Scam messages.
- Suspicious online contact.
- Inappropriate use of technology.

Concerns should be reported to:

- Class Teacher.

- Designated Safeguarding Lead.
- Headteacher.

Serious incidents will be managed in accordance with safeguarding procedures and may involve external agencies where appropriate.

Working with Parents and Carers

Longwill School recognises the importance of partnership with families.

To support this:

- An Online Safety Newsletter is distributed every term.
- The newsletter is written in accessible language.
- A QR code is included which links directly to a British Sign Language (BSL) interpretation.
- As a specialist school for deaf children, Longwill School recognises the importance of providing information in a variety of accessible formats. Online safety information, safeguarding updates and guidance for parents and carers will be communicated through ClassDojo, text messages, emails, letters, newsletters, posters and school displays. Where appropriate, information will also be supported through British Sign Language (BSL) resources to ensure that all members of the school community can access key messages about keeping children safe online.
- Parents and carers are encouraged to discuss online safety regularly with their children and to contact the school if they have any concerns.

Considering the Government's June 2026 announcement regarding social media access for children under 16, parents and carers are encouraged to carefully consider the age appropriateness of social media platforms and to follow national guidance regarding minimum age requirements and online supervision.

Use of ClassDojo

Longwill School uses ClassDojo as a secure communication platform to strengthen partnerships between school and home. ClassDojo enables staff to share learning experiences, celebrate achievements, communicate key messages and provide updates to parents and carers in a safe and controlled environment.

The use of ClassDojo supports the school's commitment to accessible communication with families and helps ensure that important information is shared promptly and effectively.

All staff using ClassDojo are expected to:

- Follow the school's safeguarding, professional conduct and acceptable use policies.
- Always communicate in a professional manner.
- Use ClassDojo solely for educational and school-related purposes.
- Protect the confidentiality and privacy of pupils and families.
- Ensure that any photographs, videos or learning updates shared through the platform comply with parental consent arrangements and GDPR requirements.

Parents and carers are expected to:

- Use ClassDojo respectfully and appropriately.
- Communicate courteously with school staff.
- Maintain the privacy of other children and families.
- Report any concerns regarding online communication to the school.

ClassDojo is used as part of the school's wider commitment to safe digital communication. The platform has been assessed by the school for suitability, safeguarding considerations and UK GDPR compliance before implementation.

As a Rights Respecting School holding the Gold UNCRC Award, Longwill School recognises the importance of ensuring that all communication platforms promote children's rights, wellbeing, safety and inclusion.

Data Protection and GDPR Compliance

Longwill School is committed to maintaining the highest standards of data protection and privacy. The school complies fully with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and all relevant safeguarding legislation.

The school recognises that the personal information of pupils, families, staff and visitors is confidential and must be always handled securely and lawfully.

Our Commitment

Longwill School will:

- Process personal data fairly, lawfully and transparently.
- Collect only the information necessary for educational, safeguarding and operational purposes.
- Ensure personal data is accurate and kept up to date.
- Store information securely using approved systems and secure networks.
- Restrict access to personal data to authorised individuals only.
- Retain information only for as long as required by law and statutory guidance.
- Dispose of records securely when they are no longer needed.
- Report any data breaches in accordance with UK GDPR requirements.

Staff Responsibilities

All staff are responsible for protecting confidential information and must:

- Complete data protection and information security training.
- Follow school policies relating to confidentiality, data protection and acceptable use.
- Use only authorised school devices, software and systems for school business.
- Lock devices when unattended.
- Keep passwords secure and never share login credentials.
- Report suspected data breaches immediately to the Headteacher or Data Protection Officer.
- Ensure that personal information is not discussed in public areas or shared with unauthorised individuals.

Use of Technology and Communication

Staff must use school-approved communication systems when communicating about pupils, families or school business.

The use of personal email accounts, social media accounts, messaging applications or personal cloud storage for school business is prohibited unless specifically authorised by the Headteacher.

Photographs, videos and recordings of pupils must only be taken using approved school equipment and in accordance with parental consent arrangements and safeguarding procedures.

Online Safety and GDPR

As part of our commitment to safeguarding and online safety, Longwill School ensures that all digital platforms, applications and online learning tools used within school are assessed for GDPR compliance before implementation.

The school will only use educational technology providers that demonstrate appropriate security measures and compliance with UK data protection requirements.

Children's Rights and Privacy

In line with the United Nations Convention on the Rights of the Child (UNCRC), particularly Article 16 (Right to Privacy), L School respects every child's right to have their personal information protected.

Pupils will be taught, through the Evolve 360 Online Safety Curriculum, how to:

- Protect their personal information online.
- Recognise phishing attempts and online scams.
- Understand privacy settings.
- Make informed choices about sharing information digitally.
- Seek support if they are concerned about their privacy or online safety.

Through robust GDPR compliance and effective online safety education, Longwill School aims to create a secure environment where pupils, families and staff can have confidence that personal information is protected and handled responsibly.

Artificial Intelligence (AI)

Longwill School recognises that Artificial Intelligence (AI) is becoming an increasingly common part of children's online experiences and educational environments. AI tools can provide valuable opportunities for learning, creativity and accessibility, particularly for deaf children, but they also present risks that require careful management.

The school is committed to ensuring that any use of AI is safe, ethical, age-appropriate and compliant with safeguarding and data protection requirements.

Teaching Children About AI

As part of the Evolve 360 Online Safety Curriculum and Computing curriculum, pupils will be taught to:

- Understand what Artificial Intelligence is and how it is used in everyday life.
- Recognise that AI-generated content may not always be accurate or trustworthy.
- Question information provided by AI systems and verify information from reliable sources.
- Understand that AI-generated images, videos and audio can be manipulated or misleading.
- Recognise scams, misinformation and fake content that may be created using AI.
- Know how to seek support if they encounter content online that causes concern.

Staff Use of AI

Staff may use approved AI tools to support professional tasks where appropriate, including planning, administration and the creation of educational resources.

However, staff must:

- Follow all safeguarding, confidentiality and GDPR requirements.
- Never input personally identifiable information relating to pupils, families or staff into public AI systems.
- Never upload confidential school documents to AI platforms unless specifically approved by the school.

- Check and verify all AI-generated content before using it in school.
- Ensure that AI-generated materials are appropriate, accurate and inclusive.
- Always exercise professional judgement.

AI must support, not replace, the professional expertise and decision-making of school staff.

Safeguarding and AI

The school recognises emerging safeguarding risks associated with AI, including:

- AI-generated scams and fraud.
- Deepfake images, videos and audio.
- Online grooming using AI-generated content.
- Misinformation and disinformation.
- AI chatbots that may provide inaccurate, inappropriate or harmful advice.

Staff will remain vigilant to these risks and will address concerns through the school's safeguarding procedures.

Accessibility and Inclusion

As a school for deaf children, L School recognises that AI technologies may provide additional accessibility benefits, including captioning, translation, transcription and communication support.

Any AI-based accessibility tools used by the school will be carefully assessed for safeguarding, GDPR compliance, accuracy and suitability before implementation.

Monitoring and Review

The school will continue to monitor developments in Artificial Intelligence and will review its practices regularly to ensure they remain aligned with safeguarding guidance, UK GDPR requirements, Department for Education guidance and best practice in online safety.

Monitoring and Review

This policy will be reviewed annually by the Headteacher, Designated Safeguarding Lead and Computing Lead.

The policy may also be reviewed following:

- Changes/updates in legislation.
- Updates to safeguarding guidance.
- Emerging online risks.
- Significant incidents.

Conclusion

Longwill School is committed to ensuring that every pupil can enjoy the benefits of technology whilst remaining safe, informed and empowered. Through a rights-respecting approach, effective safeguarding practices, partnership with families and a structured online safety curriculum, we strive to create a culture where all members of our school community use technology safely and responsibly.

Gemma Hall Computing Lead June 2026

Pupil Acceptable Use Policy

At Longwill School, we use computers, tablets and the internet to help us learn, communicate and have fun safely.

To help keep everyone safe, I agree to follow these rules:



I



will

✓ Ask a teacher before using a computer, tablet or other technology.

✓ Only use websites, apps and activities that a teacher has told me or allowed me to use.

✓ Take care of computers, tablets and equipment.

✓ Use technology respectfully and kindly.

✓ Keep my passwords private and not share them with friends.

✓ Ask a teacher if I am unsure what to do.

✓ Tell a teacher or trusted adult if I see something online that upsets me, worries me or makes me feel uncomfortable.

✓ Tell a member of staff if someone is unkind online.

✓ Use my own account and not try to use someone else's account.

✓ Be kind and respectful when communicating online.

✓ Remember that not everything I see online is true.

✓ Ask an adult before sharing any personal information online.

✓ Use technology in a way that follows our school values and our Rights Respecting School principles.



Article 17: I have the right to access information.

Article 36: I have the right to be kept safe from things that could harm me.



I



will not

X Be unkind, rude or hurtful to others online.

X Take photographs or videos of other people without permission.

X Deliberately search for or access inappropriate content.

X Use Artificial Intelligence (AI) tools unless a teacher has given permission and is helping me to use them safely.

If Something Goes Wrong

If I accidentally see something upsetting or inappropriate:



I



will

✓ I will stop using the device.

✓ I will tell a teacher or trusted adult straight away.

✓ I know I will not get into trouble for reporting it.

Mobile Phones



Mobile phone

If I bring a mobile phone to school:

✓ I will hand it in to the office.

I understand that these rules help keep me and others safe.

I know that if I do not follow these rules, I may not be allowed to use school computers, tablets, the internet or other technology.

Pupil signature: _____



I



promise

Pupil name: _____

Class: _____

Date: _____



Article 17: I have the right to access information.

Article 36: I have the right to be kept safe from things that could harm me.

Add CIP differentiated AUP – once standard is signed off by SMT

Jess do you want this removed?

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

Jess risk assessment on next page - it was complete by AC - I think maybe it needs updating with GDPR and AI to link in with the policy – I am not sure if this is something I should update or is something you need to do?

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

