



Implementation Date	September 2026
Review Date	September 2029
Reviewer	Liam Donovan

E-Safety Policy

1. Purpose

Longwood School & Nursery recognises that technology is an important part of children's education and everyday life.

We aim to ensure that children, staff, parents and visitors understand how to use technology safely, responsibly and respectfully.

This policy applies to the use of computers, tablets, phones, the internet, email, online platforms, social media, artificial intelligence (AI) and other digital technologies used in or connected with the school.

2. Our aims

We aim to:

- Keep children safe when using technology and the internet.
- Teach children how to recognise and manage online risks.
- Encourage responsible and respectful online behaviour.
- Support staff in using technology safely and appropriately.
- Help parents and carers understand how they can support children's online safety.
- Respond appropriately to online safety concerns or incidents.

3. Children

Children are taught age-appropriate online safety as part of the curriculum and through everyday teaching.

Children are encouraged to:

- Tell a trusted adult if something online worries or upsets them.
- Be kind and respectful when communicating online.

- Keep personal information private.
- Use appropriate usernames, passwords and security measures where relevant.
- Check with an adult before accessing unfamiliar websites, apps or online content.
- Understand that not everything online is true or suitable.
- Report inappropriate or unsafe content.
- Never arrange to meet someone they have only met online.

The school will provide additional support where a child needs help managing an online safety issue.

4. Staff

Staff are expected to:

- Use school technology and online services appropriately.
- Follow the school's Acceptable Use arrangements.
- Keep passwords and personal information secure.
- Avoid accessing inappropriate or unsuitable content using school equipment or networks.
- Use professional judgement when communicating with children and families online.
- Report online safety concerns to the Designated Safeguarding Lead (DSL).
- Take care when using personal devices in school.
- Follow school guidance when using AI or other emerging technologies.

Staff should not communicate with pupils through personal social media accounts or personal messaging services.

5. Filtering and monitoring

The school will take reasonable steps to provide appropriate filtering and monitoring of internet use.

The school recognises that filtering and monitoring cannot remove every online risk. Staff remain responsible for supervising children and responding to concerns.

The school will review its filtering and monitoring arrangements regularly and make changes where necessary.

6. Personal devices

Children should only use personal devices in school when this has been authorised by the school.

Staff should use personal devices responsibly and in accordance with school procedures.

Personal mobile phones should not be used to photograph or record children unless specifically authorised as part of school procedures.

7. Social media

Staff, pupils and parents/carers are expected to use social media responsibly.

Staff must maintain professional boundaries and must not post information, photographs or comments about pupils or the school that could compromise confidentiality, safeguarding or the reputation of the school.

Parents and carers are asked not to post photographs, videos or personal information about other children without appropriate permission.

Concerns about the school or individual members of staff should be raised directly with the school rather than through social media.

8. Cyberbullying

The school does not tolerate bullying or harassment carried out through digital technology.

This includes:

- Hurtful or threatening messages.
- Sharing embarrassing photographs or videos.
- Excluding someone from online groups.
- Creating false accounts or impersonating others.
- Spreading rumours online.
- Sending abusive or inappropriate content.

Any concerns about cyberbullying should be reported to a member of staff.

The school will respond in accordance with its safeguarding and behaviour procedures.

9. Personal information and photographs

The school will handle personal information in accordance with its data protection responsibilities.

Photographs and videos of children will only be taken, stored and shared in accordance with school procedures and relevant permissions.

Children should not be identified or have personal information shared online inappropriately.

10. Artificial Intelligence (AI)

The school recognises that AI is developing quickly and may be used in education and everyday life.

Staff and pupils should use AI responsibly and safely.

AI must not be used to:

- Share confidential or personal information.
- Create harmful, offensive or inappropriate material.
- Replace professional judgement where safeguarding or children's welfare is involved.
- Produce or share content that could cause harm to others.

The school will review its approach to AI as technology and guidance develop.

11. Reporting concerns

Anyone who has an online safety concern should report it to a member of staff.

Safeguarding concerns should be reported to the **Designated Safeguarding Lead (DSL)** in accordance with the school's safeguarding procedures.

Where appropriate, the school may work with parents/carers, the Local Authority, police or other relevant organisations.

12. Parents and carers

The school encourages parents and carers to:

- Talk regularly with their child about online safety.
- Set appropriate boundaries for technology use at home.
- Know which apps, games and websites their child uses.
- Use parental controls where appropriate.
- Encourage children to tell them about anything that worries them online.
- Report significant online safety concerns to the school where appropriate.

The school will provide information and guidance to parents and carers where possible.

13. Training and review

Staff will receive appropriate online safety information and training.

The school will review this policy regularly and update it when necessary to reflect:

- Changes in technology.
- Changes in legislation or national guidance.
- Changes to school procedures.
- Lessons learned from online safety incidents.

14. Related policies

This policy should be read alongside relevant school policies, including:

- Safeguarding and Child Protection Policy.
- Behaviour Policy.
- Data Protection / Privacy Policy.
- Staff Code of Conduct.
- Acceptable Use Policy.
- Anti-Bullying Policy.
- Remote Learning Policy, where applicable.

15. Review

This policy will be reviewed at least annually, or sooner if there are significant changes to legislation, guidance, technology or school practice.