



Wavell Community Primary School

Internet Safety Policy

Academic Year 2026-2027

Approved by: Governing Board

Review Date: Annually

Responsible Person: Headteacher/Designated Safeguarding Lead (DSL)/Computing Lead

1. Policy Statement

At Wavell Community Primary School, we recognise that digital technologies and the internet are an essential part of modern life and learning. We are committed to ensuring that all children, staff, governors, volunteers and visitors use technology safely, responsibly and effectively.

Online safety is a safeguarding issue. The school adopts a proactive, whole-school approach to promoting safe and responsible use of technology and educating pupils about the benefits, risks and responsibilities associated with the online world. This policy supports our safeguarding ethos and our commitment to ensuring that every child is safe, respected and able to thrive in an increasingly digital society.

Our approach reflects our school vision to **"Be the Best You"** and supports our curriculum drivers of **A Healthy, Happy Me, Learning for Life, Talk to Me, Listen to Me, and My Place in the World**. These drivers are embedded throughout our online safety curriculum and wider safeguarding provision.

2. Aims

The aims of this policy are to:

- Safeguard and protect all members of the school community online.
- Promote the safe, responsible and respectful use of digital technologies.
- Educate pupils about online risks and how to respond appropriately.
- Support parents and carers in keeping children safe online.
- Establish clear expectations for the use of technology within school.
- Ensure effective procedures are in place for responding to online safety concerns.
- Comply with statutory safeguarding requirements and relevant legislation.

3. Legal Framework

This policy should be read alongside:

- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- UK GDPR and Data Protection Act 2018
- Education Act 2002
- Prevent Duty Guidance
- Searching, Screening and Confiscation Guidance
- Behaviour Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Acceptable Use Agreements
- Remote Learning Policy

4. Scope

This policy applies to:

- All children
- All staff
- Governors
- Volunteers
- Visitors
- Contractors working on behalf of the school

The policy covers use of:

- Internet-enabled devices
- School networks
- Mobile phones
- Tablets
- Digital cameras
- Educational technologies
- Social media
- Cloud-based services
- Artificial Intelligence (AI) tools

5. Roles and Responsibilities

Governing Board

The Governing Board will:

- Ensure appropriate online safety arrangements are in place.
- Monitor the effectiveness of this policy.

- Receive regular safeguarding and online safety updates.
- Ensure filtering and monitoring systems are effective and appropriate.

Headteacher

The Headteacher will:

- Promote a strong culture of online safety.
- Ensure staff receive appropriate training.
- Oversee the implementation of this policy.
- Ensure identified online safety concerns are addressed promptly.

Designated Safeguarding Lead (DSL)

The DSL will:

- Lead on online safety as part of safeguarding responsibilities.
- Manage online safety incidents and referrals.
- Maintain records of concerns.
- Liaise with parents, external agencies and the Local Authority where appropriate.
- Monitor emerging online safeguarding risks.

Staff

All staff will:

- Model safe and professional use of technology.
- Teach online safety through the curriculum.
- Report concerns immediately using school safeguarding procedures.
- Maintain professional boundaries online.
- Follow the school's Acceptable Use Agreement.

Children

Children are expected to:

- Use technology responsibly.
- Respect others online.
- Protect personal information.
- Report anything that makes them feel uncomfortable, worried or unsafe.
- Follow school rules for the safe use of technology.

Parents and Carers

Parents and carers are encouraged to:

- Promote safe online behaviour at home.

- Monitor children's online activity.
- Inform school of any concerns which may impact upon a child's wellbeing or safety.
- Work in partnership with the school to reinforce key online safety messages.

6. Teaching and Learning

Online safety is taught as part of our Computing, PSHE and RSHE curriculum and is reinforced throughout school life.

Children are taught:

Early Years Foundation Stage

- Basic rules for using technology safely.
- Asking trusted adults for help.
- Understanding that information online may not be safe.

Key Stage 1

- Keeping personal information private.
- Using devices safely.
- Seeking help when worried.
- Kind and respectful online behaviour.

Key Stage 2

- Digital footprints.
- Privacy settings.
- Cyberbullying.
- Online relationships.
- Fake news and misinformation.
- Social media awareness.
- Gaming safety.
- Online scams.
- Age restrictions.
- Responsible use of AI and emerging technologies.

The curriculum is age-appropriate, inclusive and reflects current safeguarding risks, including social media use and wider community online safety concerns identified by school leaders.

7. Cyberbullying

The school takes all forms of bullying seriously, including cyberbullying.

Cyberbullying may include:

- Sending threatening messages.

- Sharing inappropriate images.
- Excluding others online.
- Creating fake profiles.
- Deliberately humiliating or intimidating others through digital technologies.

Incidents will be investigated in line with the Behaviour Policy and Safeguarding Policy.

8. Use of School Devices and Network

The school provides filtered and monitored internet access.

Users must:

- Only access age-appropriate and educational content.
- Use their own login credentials.
- Keep passwords secure.
- Report accidental access to unsuitable material.
- Use equipment responsibly.

Users must not:

- Access inappropriate content.
- Attempt to bypass filtering systems.
- Download unauthorised software.
- Share passwords.
- Use school systems for illegal or offensive purposes.

9. Filtering and Monitoring

The school maintains robust filtering and monitoring arrangements to protect pupils from harmful content. (Smoothwall supported by NYES Digital)

Systems are designed to:

- Restrict access to inappropriate material.
- Monitor online activity.
- Alert leaders to potential safeguarding concerns.
- Support compliance with statutory guidance.

Filtering and monitoring arrangements are reviewed regularly by leaders and governors as part of safeguarding oversight. Online safety remains a strategic safeguarding priority within school improvement planning.

10. Social Media

Staff

Staff must:

- Maintain professional boundaries at all times.
- Never communicate with pupils through personal social media accounts.
- Ensure privacy settings are appropriate.
- Follow the Staff Code of Conduct.

Children

Children must not:

- Access age-restricted social media platforms.
- Share personal information.
- Post harmful or inappropriate content.

Parents

The school asks parents and carers to:

- Communicate concerns directly with the school.
- Avoid posting images or information that may compromise the safety or privacy of children.
- Support the school's online safety messages.

11. Artificial Intelligence (AI)

The school recognises the growing use of AI technologies.

Where AI tools are used:

- They will support learning and teaching appropriately.
- Pupils will be taught to question information critically.
- Personal data must not be entered into public AI systems without authorisation.
- Staff will follow school guidance regarding acceptable AI use.

12. Online Safety Incidents

Any online safety concern will be treated as a safeguarding matter where appropriate.

Concerns may include:

- Cyberbullying
- Child-on-child abuse
- Online exploitation
- Exposure to harmful content
- Radicalisation
- Online grooming
- Sextortion

- Sharing indecent images
- Inappropriate contact from unknown individuals

All concerns should be reported immediately to the DSL.

Where necessary, the school will work with:

- Parents and carers
- Children's Social Care
- Police
- The Local Authority
- CEOP

13. Data Protection and Privacy

The school is committed to protecting personal information and complying with UK GDPR.

Staff will:

- Handle data securely.
- Follow school data protection procedures.
- Report any suspected data breaches immediately.

14. Training

The school will ensure:

- All staff receive regular online safety training.
- Governors receive safeguarding updates, including online safety.
- Parents receive information and guidance through newsletters, workshops and school communications.
- Online safety messages are revisited throughout the year.

15. Monitoring and Review

This policy will be reviewed annually, or sooner if:

- National legislation changes.
- Safeguarding guidance is updated.
- New technologies create emerging risks.
- School circumstances require amendment.

The Governing Board will receive regular reports regarding online safety, safeguarding trends and the effectiveness of school systems.

Appendix 1: Child-Friendly Online Safety Rules

At Wavell Community Primary School, we:

1. Keep personal information private.
2. Tell a trusted adult if something worries us online.
3. Use kind words online.
4. Only visit websites approved by adults.
5. Never share passwords.
6. Think before we post.
7. Respect other people online.
8. Stop, close and tell an adult if something makes us feel unsafe.
9. Use technology responsibly.
10. Always try to "Be the Best You" online and offline.