



Online Safety Policy 2026-2027

Date Reviewed: September 2026

Review Date: September 2027

Approved by H&S Governors: September 2026

Key Personnel

Role	Name
Designated Safeguarding Lead (DSL)	R Cook (Headteacher)
Online Safety Lead	C Squires (Class teacher)
Deputy DSL	K. Byrne-Corbett (Pastoral Manager)
Deputy DSL	P. Titley (Deputy Nursery Manager)
Deputy DSL	M. Shayes (Class Teacher/CIC Lead)
Deputy DSL	C McFarland (SENDco & AHT)
Safeguarding Governor	R. Penwright
Online Safety & Cyber Security Governor	D. Shorter
Computing Lead	C Squires
RSHE Leads	L. Churm (Teacher)
Network Support	D. Clarke (T&W IDT)
Data Protection Officer	R. Montgomery

Policy Statement

At Newdale Primary School, we recognise that technology plays an important role in children's learning, communication and daily lives. We are committed to creating a culture where pupils can use technology safely, responsibly and positively.

Online safety is a safeguarding issue and is everyone's responsibility. The online world presents many opportunities for learning and personal development but can also expose children to risks, including inappropriate content, harmful contact, cyberbullying, online abuse, exploitation and misinformation.

This policy supports the school's commitment to safeguarding and promoting the welfare of all children and should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Cyber Security Policy
- Acceptable Use Agreements (AUPs)

Aims

This policy aims to:

- Safeguard pupils when using digital technologies.
- Promote safe, responsible and respectful online behaviour.
- Develop pupils' digital resilience and critical thinking skills.
- Support staff, governors and parents in understanding their online safety responsibilities.
- Ensure effective filtering and monitoring arrangements.
- Provide clear processes for responding to online safety concerns.
- Promote positive digital wellbeing for all members of the school community.

Scope

This policy applies to all members of the Newdale Primary School community, including:

- Pupils
- Staff
- Governors
- Volunteers
- Contractors
- Visitors
- Parents and carers

The policy applies whenever technology is used for school-related purposes, whether on school premises or elsewhere.

Roles and Responsibilities

Governing Body

Governors will:

- Monitor the effectiveness of online safety arrangements.
- Ensure statutory safeguarding requirements are met.
- Receive regular safeguarding and online safety updates.
- Provide challenge and support regarding filtering, monitoring and cyber security.

Headteacher

The Headteacher will:

- Ensure effective implementation of this policy.
- Promote a strong safeguarding culture.

- Ensure appropriate staff training is in place.
- Oversee filtering and monitoring arrangements.

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety and will:

- Manage online safety incidents.
- Work with technical staff regarding filtering and monitoring.
- Ensure safeguarding records are maintained.
- Deliver or coordinate staff training.
- Review the effectiveness of online safety procedures.

Staff

All staff will:

- Model safe and professional online behaviour.
- Follow the Acceptable Use Policy.
- Monitor pupils' use of technology.
- Report concerns immediately using safeguarding procedures.

Parents and Carers

Parents and carers are expected to:

- Support their child's safe use of technology.
- Engage with school guidance and advice.
- Report concerns that may impact a child's welfare.

Pupils

Pupils are expected to:

- Follow the Pupil Acceptable Use Agreement.
- Use technology responsibly.
- Treat others respectfully online.
- Report anything that concerns or upsets them.

Online Safety Education

Online safety is embedded throughout the curriculum and wider school life.

Teaching takes place through:

- Computing
- RSHE
- PSHE (Life Learning lessons)
- Assemblies
- Safer Internet Day activities
- Cross-curricular opportunities

Pupils are taught about:

- Online relationships
- Personal information and privacy
- Cyberbullying
- Digital footprints
- Social media awareness
- Online gaming
- Misinformation and disinformation
- Online scams
- Healthy screen use
- Safe use of artificial intelligence
- Reporting concerns and seeking help

The school uses the UK Council for Internet Safety's *Education for a Connected World Framework* to support progression in learning.

Digital Wellbeing

Newdale Primary School promotes healthy and balanced use of technology.

Pupils are encouraged to:

- Balance screen time with other activities.
- Develop healthy online habits.
- Understand the impact of excessive screen use on wellbeing.
- Build positive relationships both online and offline.

We recognise the importance of positive role modelling by adults and encourage partnership working with parents to support healthy technology use.

Artificial Intelligence (AI)

The school recognises the increasing use of generative AI technologies.

Staff and pupils will be educated about:

- Benefits and limitations of AI
- Misinformation and deepfakes

- Online scams and manipulation
- Privacy and data protection risks
- Ethical use of AI

Any AI tools used within school must:

- Be appropriate for the age of pupils.
- Support learning outcomes.
- Be approved by school leaders.
- Comply with safeguarding and data protection requirements.

Personal or sensitive pupil information must never be entered into public AI systems.

Filtering and Monitoring

Newdale Primary School has appropriate filtering and monitoring systems in place to help keep children safe online.

Current systems include:

- **Lightspeed Filtering**
- **SENSO Monitoring**

The DSL has lead responsibility for filtering and monitoring and works closely with technical support staff to ensure systems meet Department for Education standards.

The school will:

- Review filtering and monitoring arrangements regularly.
- Investigate concerns raised by monitoring systems.
- Record incidents in line with safeguarding procedures.
- Ensure staff understand their responsibilities regarding filtering and monitoring.

Safe Search is enabled on all school-managed devices.

Managing Online Safety Concerns

Online safety concerns are treated as safeguarding concerns.

All staff must:

- Remain vigilant.
- Act immediately.
- Report concerns to the DSL on the same day.
- Record concerns using the school's safeguarding system – CPOMS.

Concerns may include:

- Cyberbullying
- Online abuse
- Grooming or exploitation
- Extremism or radicalisation
- Exposure to inappropriate content
- Sharing of nude or semi-nude images
- Sexual harassment
- AI-generated harmful content
- Online scams or financial exploitation

The school will work with parents, external agencies and the police where appropriate.

Remote Learning and Online Communication

Where learning takes place remotely, the school will ensure that:

- Approved platforms are highlighted to parents.
- Appropriate safeguarding measures are followed.
- Pupils know how to report concerns.
- Staff maintain professional boundaries at all times.

Sharing Nude or Semi-Nude Images

The school follows UK Council for Internet Safety (UKCIS) guidance regarding incidents involving nude or semi-nude images.

Staff must:

- Never view, forward or save images.
- Never ask a pupil to produce or share images.
- Report concerns immediately to the DSL.

The DSL will determine appropriate action and whether external agencies need to be involved.

Cyberbullying

Cyberbullying is taken seriously and will be dealt with in accordance with the Behaviour and Anti-Bullying Policies.

Examples include:

- Abusive messaging
- Excluding others online

- Sharing harmful content
- Creating fake profiles
- Filming or sharing incidents without permission

Support will be provided to all parties involved.

Social Media

Members of the school community are expected to use social media responsibly.

The school does not tolerate:

- Harassment or intimidation
- Inappropriate comments about pupils, staff or families
- Sharing confidential information
- Posting images without permission

Where social media activity presents a safeguarding concern, the matter will be investigated and addressed through appropriate procedures.

Photography and Video

Photographs and videos of pupils will only be taken, stored and used in accordance with:

- Parental permissions
- Data protection legislation
- School procedures

The school will:

- Regularly review consent records.
- Avoid identifying pupils by full name in public-facing materials.
- Store images securely.

Parents and visitors must seek permission before taking photographs or videos on school premises e.g. during school performances.

The filming or live-streaming of staff, pupils or parents without permission is not permitted.

Mobile Phones and Personal Devices

Pupils

Pupils who bring mobile phones to school must hand them to the school office upon arrival.

Phones will be returned at the end of the school day.

Pupils must not:

- Use mobile phones during the school day.
- Photograph or record others without permission.
- Use devices in a way that causes disruption or harm.

Staff

Staff should keep personal phones on silent and use them only in designated staff areas. They may only be accessed in cases of emergency e.g. if a lockdown is activated and then they may access the emergency 'Quantum' Whatsapp group.

Staff must not:

- Store school data on personal devices.
- Communicate with pupils through personal accounts.
- Use personal devices inappropriately whilst supervising pupils.

Visitors, Volunteers and Contractors

Personal devices should not be used around pupils unless authorised by the Headteacher.

Cyber Security and Data Protection

The school recognises the strong link between cyber security and safeguarding.

The school follows DfE Cyber Security Standards and promotes:

- Strong passwords
- Multi-factor authentication where available
- Secure storage of data
- Appropriate access controls
- Regular software updates
- Reporting of suspicious activity

The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information where there is a safeguarding concern.

Protecting children will always be the priority.

17. Breaches of this Policy

Any misuse of technology may result in:

- Loss of access to school technology
- Behaviour sanctions
- Safeguarding intervention
- Parent meetings
- Referral to external agencies where appropriate
- Disciplinary action for staff

Serious incidents may be referred to the police or other statutory agencies.

Monitoring and Review

This policy will be reviewed annually by:

- Headteacher
- Designated Safeguarding Lead
- Online Safety Lead
- Governing Body

The policy may also be reviewed sooner if required by changes in legislation, safeguarding guidance or school practice.

This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy and Acceptable Use Agreements.