

Online Safety Policy

A policy for all stakeholders

Date of last review:	July 2026	Author:	Bernadette O'Rourke Head of School
Date of next review:	September 2027	Owner:	Brookfields Primary School Bernadette O'Rourke Head of School/ Safeguarding Lead
Type of policy:	Applicable to all stakeholders	Approval:	LAB/Trust
School:	Brookfields Primary School	Key Contact Name:	Bernadette O'Rourke Head of School/ Safeguarding Lead
Key contact email:	enquiry@brookfields.create.org.uk safeguarding@brookfields.create.org.uk	Version:	1.2

This policy is reviewed annually by the school. As part of the review process, consideration will be given to feedback from pupils, parents/carers, staff, governors and other stakeholders. Feedback gathered through pupil voice activities, meetings, surveys and stakeholder engagement will be used, where appropriate, to inform future revisions and ensure the policy continues to meet the needs of the Brookfields community.

Brookfields Primary School

Online Safety Policy 2026–2027

1. Aims

At Brookfields Primary School, safeguarding and promoting the welfare of children is our highest priority. We recognise that technology and the internet are an integral part of children's lives, learning and future opportunities. We are committed to ensuring that all pupils learn to use digital technology safely, responsibly, respectfully and confidently. Online safety is an essential component of safeguarding and forms part of our wider culture of child protection and wellbeing.

This policy aims to:

- *Protect children from online risks and harms.*
- *Ensure pupils use technology safely, responsibly and respectfully.*
- *Develop pupils' digital resilience, critical thinking skills and media literacy.*
- *Establish clear procedures for preventing, identifying and responding to online safety concerns.*
- *Promote a whole-school culture where online safety is everyone's responsibility.*
- *Support parents and carers in promoting safe online behaviours.*
- *Ensure effective filtering and monitoring arrangements are in place.*
- *Provide staff with the knowledge and training needed to safeguard children in a digital world.*

The Four Areas of Online Risk:

Our approach to online safety is based on addressing four key categories of risk:

Content – exposure to illegal, inappropriate or harmful content, including misinformation, disinformation, fake news, extremism and harmful material.

Contact – harmful online interactions, including grooming, exploitation, coercion and inappropriate contact.

Conduct – unsafe or inappropriate online behaviour, including cyberbullying, sharing images, harassment and misuse of technology.

Commerce – risks associated with scams, phishing, gambling, financial exploitation and inappropriate advertising.

2. Legislation and Guidance

This policy is based upon and informed by:

- Keeping Children Safe in Education (KCSIE)
- Teaching Online Safety in Schools
- Relationships Education and Health Education guidance
- Cyberbullying: Advice for Headteachers and School Staff
- Preventing and Tackling Bullying
- Searching, Screening and Confiscation
- Prevent Duty Guidance
- Education Act 1996
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011.

3. Roles and Responsibilities

3.1 Governing Board

The Governing Board has overall responsibility for monitoring this policy and ensuring the effectiveness of online safety arrangements.

Governors will:

- Ensure robust safeguarding arrangements are in place.
- Ensure appropriate filtering and monitoring systems are operational.
- Monitor the implementation and effectiveness of this policy.
- Receive regular reports on online safety.
- Ensure staff receive appropriate online safety training.
- Ensure online safety is embedded within the school's safeguarding culture.

3.2 Head of School/

The Headteacher is responsible for:

- Ensuring this policy is implemented consistently.
- Establishing a positive culture of safeguarding and online safety.
- Supporting the DSL in managing online safety concerns.
- Ensuring staff understand their safeguarding responsibilities.

3.3 Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety and will:

- Lead online safety across the school.
- Respond to concerns identified through filtering and monitoring.
- Manage online safety incidents.
- Maintain records of online safety concerns.
- Deliver staff training and updates.
- Liaise with external agencies where required.
- Provide reports to senior leaders and governors.
- Undertake annual risk assessments relating to online safety.
- Share weekly online safety updates in the staff newsletter

Brookfields Primary School's Lead DSL is the Deputy Headteacher, Bernadette O'Rourke.

3.4 ICT Support

The school's ICT support provider is responsible for:

- Maintaining secure systems and networks.
- Applying security updates and malware protection.
- Managing filtering and monitoring systems.
- Reporting technical safeguarding concerns.
- Supporting investigations into online safety incidents.

3.5 Staff and Volunteers

All staff and volunteers must:

- Read and follow this policy.
- Promote safe and responsible technology use.
- Report concerns immediately to the DSL.
- Maintain awareness of emerging online risks.
- Understand their responsibilities regarding filtering and monitoring.
- Complete required safeguarding and online safety training.

3.6 Parents and Carers

Parents and carers are expected to:

- Support safe technology use at home.
- Encourage positive online behaviour.
- Report concerns to the school.
- Work in partnership with the school to safeguard children online.

4. Educating Pupils About Online Safety

Online safety is embedded throughout the curriculum and wider safeguarding culture of Brookfields Primary School.

Online safety is taught through:

- Computing lessons
- PSHE
- Relationships Education
- Assemblies
- Safer Internet Day activities
- Cross-curricular opportunities
- Safeguarding awareness events.

Key Stage 1

Pupils are taught to:

- Use technology safely and respectfully.
- Keep personal information private.
- Identify trusted adults who can help them.
- Recognise when something online makes them feel worried or unsafe.

Key Stage 2

Pupils are taught to:

- Use technology safely, responsibly and respectfully.
- Evaluate online information critically.
- Understand social media age restrictions.
- Recognise cyberbullying and know how to report concerns.
- Protect personal information and privacy.
- Understand online relationships and safe communication.
- Identify misinformation, fake news and manipulated content.

Pupils will also learn about:

- Online grooming and exploitation.
- Online gaming risks.
- Sharing photographs and personal content safely.
- Digital footprints.
- Respectful online behaviour.
- Artificial intelligence and AI-generated content.
- How and when to seek help.

Teaching is age-appropriate and responsive to emerging technologies and current online risks.

5. Filtering and Monitoring

Brookfields Primary School maintains appropriate filtering and monitoring systems to safeguard pupils when using school devices, networks and online services.

These systems:

- Help prevent access to harmful, inappropriate or illegal content.
- Support the identification of safeguarding concerns.
- Alert relevant staff where risks are identified.
- Are reviewed regularly to ensure effectiveness and proportionality.

Senior leaders, governors and safeguarding leaders maintain oversight of filtering and monitoring arrangements.

Whilst no filtering or monitoring system can guarantee complete protection, the school takes all reasonable steps to minimise risk.

6. Educating Parents and Carers

Parents and carers play a vital role in helping children stay safe online.

The school supports families through:

- Newsletters and safeguarding updates.
- Parent workshops and information sessions.
- Guidance on parental controls.
- Advice on age ratings and social media platforms.
- Information about emerging online risks.
- Resources available through the school website.

Parents are encouraged to maintain open conversations with children about their online experiences and to contact the school with any concerns.

7. Cyberbullying

Definition

Cyberbullying is bullying that takes place through digital technologies including social media, online gaming platforms, websites, messaging services and mobile devices.

Prevention

Brookfields Primary School adopts a zero-tolerance approach to cyberbullying.

Pupils are taught:

- What cyberbullying is.
- How to recognise it.
- How to report concerns.
- How to support others experiencing cyberbullying.

All reported incidents will be investigated and addressed in accordance with the school's Behaviour Policy and Child Protection and Safeguarding Policy.

8. Artificial Intelligence (AI)

Brookfields Primary School recognises the educational benefits of artificial intelligence (AI) while also understanding the risks it may present.

The school will:

- Promote responsible use of AI technologies.
- Teach pupils to critically evaluate AI-generated content.
- Raise awareness of misinformation, fake content and deepfakes.
- Support pupils in understanding how AI can be used safely and ethically.
- Address any misuse of AI as a safeguarding or behaviour concern where appropriate.

Any use of AI to bully, harass or deceive others will be treated seriously and managed in line with safeguarding and behaviour procedures.

9. Acceptable Use of Technology

All members of the school community are expected to:

- Use technology responsibly.
- Protect passwords and personal information.
- Respect others online.
- Access only appropriate content.
- Follow school acceptable use agreements.
- Report concerns immediately.

The school reserves the right to monitor the use of its systems where necessary to safeguard pupils and protect school systems.

10. Mobile Phones and Personal Devices

Pupils may bring a mobile phone to school only where necessary for travel or safety reasons.

Where a mobile phone is brought to school:

- It must remain switched off throughout the school day.
- It must not be used during lessons or break times.
- It should be handed in or stored securely in accordance with school procedures.

Any misuse of a personal device may result in confiscation and further action in line with the Behaviour Policy.

11. Staff Use of Devices

Staff using school devices outside school must:

- Keep devices password protected.
- Store information securely.
- Maintain confidentiality.
- Install updates promptly.
- Report security concerns immediately.
- Follow data protection requirements at all times.

12. Responding to Concerns

Any online safety concern is treated as a safeguarding concern.

Concerns will be:

- Recorded and reported to the DSL.
- Managed in accordance with the Child Protection and Safeguarding Policy.
- Investigated and responded to appropriately.
- Referred to external agencies where required.

This includes concerns relating to:

- Cyberbullying
- Child-on-child abuse
- Online grooming
- Exploitation
- Harmful sexual behaviour
- Radicalisation
- Extremist content
- Online scams and criminal activity.

The school will work closely with families to support children affected by online safety concerns.

13. Training

All staff receive regular online safety training as part of the school's safeguarding programme.

Training includes:

- Online abuse and exploitation.
- Cyberbullying.
- Radicalisation and extremism.
- Social media risks.
- Emerging technologies.
- Artificial intelligence.
- Recording and reporting concerns.
- Links between online behaviour and wider safeguarding issues.

Online safety is regularly discussed through safeguarding briefings, updates and professional development activities.

14. Monitoring and Review

This policy will be reviewed annually by the Headteacher and Lead DSL and approved by the Governing Board.

Additional reviews may take place following:

- Changes in legislation or national guidance.
- Significant safeguarding incidents.
- Changes in technology or identified risks.
- Changes to school procedures.

Related Policies

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Relationships Education Policy
- Computing Policy
- Complaints Procedure.

Statement of Commitment

Brookfields Primary School is committed to creating a culture where children can learn, explore and thrive safely online. Online safety is embedded throughout our safeguarding culture, curriculum and daily practice, ensuring that every child is equipped to make safe, responsible and informed choices in an increasingly digital world.

*For advice or support regarding online safety, parents and carers should contact **Bernadette O'Rourke, Head of School and Lead Designated Safeguarding Lead**, through the school office.*

Contact:

enquiry@brookfields.create.org.uk

or

safeguarding@brookfields.create.org.uk