Community Academies Trust

Birchwood Primary School Policy

Online Safety Policy

Document Reference Number (if already used)	
Title	Online Safety Policy
Policy Owner	Headteacher
Version	1.
Approved Date	March 2026
Approving Body	Governing Body
Next Review Date	March 2028

Version Control

Version	Last Modified	Last Modified By	Document Changes
1.	30.1.26	Neil Coleman	Section changes include: Inclusion, Professional Development and Inspectorate Expectations.

Table of Contents

1. Introduction

This Online Safety Policy sets out the principles, statutory requirements, and practical approaches for ensuring all pupils at Birchwood are equipped to use technology safely, respectfully, and responsibly. The policy is rooted in the 2014 National Curriculum for Computing, statutory safeguarding guidance, and the expectations of the national inspectorate. It reflects a whole-school commitment to embedding online safety across the curriculum, safeguarding culture, and wider school community, ensuring all staff, pupils, and parents understand their roles in promoting and maintaining a safe online environment.

2. Aims

Birchwood understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

- To safeguard and promote the welfare of all pupils in their use of digital technologies.
- To ensure all pupils develop age-appropriate knowledge, skills, and behaviours for safe, respectful, and responsible online activity.
- To empower pupils to recognise and respond to online risks, including cyberbullying, privacy breaches, and inappropriate content or contact.
- To foster critical thinking and resilience in navigating digital environments.
- To ensure staff are confident and competent in delivering online safety education and responding to incidents.
- To actively engage parents and carers in supporting online safety at home.
- To create an inclusive online safety curriculum accessible to all pupils.

3. Statutory Requirements

- Deliver online safety as a core element of safeguarding, in line with Keeping Children Safe in Education (KCSIE) and the Education Act 2002.
- Teach all aspects of online safety required by the 2014 National Curriculum for Computing at Key Stages 1 and 2.
- Comply with the Equality Act 2010 and SEND Code of Practice to ensure accessibility and inclusion.
- Protect pupil data and educate about privacy, in accordance with the Data Protection Act 2018 and UK GDPR.
- Fulfil the Prevent Duty by addressing online radicalisation and extremism.
- Implement statutory Relationships Education and Health Education guidance, including online relationships, cyberbullying, and privacy.
- Maintain robust filtering, monitoring, and reporting systems to provide a safe online environment.

4. Curriculum Coverage

Online safety at Birchwood is delivered through a broad, progressive curriculum that covers:
- Safe considerate and respectful use of technology, including understanding digital footprints and privacy.
- Recognising, avoiding, and reporting online risks such as cyberbullying, grooming, and exposure to inappropriate content.
- Responsible online behaviour, including managing online relationships and digital reputation.
- Identifying and responding to unacceptable behaviour and online abuse.
- Evaluating the reliability of online information and recognising misinformation.
- Understanding the importance of protecting personal information and data security.
- Awareness of the impact of online activity on wellbeing and mental health.
- Knowledge of where and how to seek help and support for online concerns.
- Cross-curricular links with PSHE, safeguarding, and RSE to reinforce key messages.

5. Curriculum Implementation

- Online safety is embedded across computing, PSHE, and safeguarding curricula using a spiral model to revisit and deepen understanding.
- Lessons are planned to be age-appropriate, progressive, and responsive to emerging risks and technologies.
- Active learning strategies, including scenario-based discussions, role play, and peer-led activities, are used to develop critical thinking and problem-solving skills.
- Pupil voice is promoted through surveys, digital leaders, school council and circle times.
- Resources are regularly updated to reflect current risks and best practice, drawing on guidance from national bodies (e.g., Childnet, CEOP).
- Online safety messages are reinforced through assemblies, themed weeks, and displays.
- Parents are engaged through workshops, newsletters, and access to online resources.
- Clear procedures are in place for reporting, recording, and responding to online safety incidents.

6. Assessment

- Formative assessment is conducted through class discussions, scenario responses, and pupil reflections.
- Summative assessment includes demonstration of safe online behaviours, completion of online safety tasks, and pupil self-assessment.
- Pupil understanding is monitored through surveys and feedback, informing curriculum development.
- Assessment outcomes are used to identify gaps in knowledge and inform targeted interventions.

7. Roles and Responsibilities

Role	Responsibilities
Governors	- Ensure statutory compliance and oversight of online safety provision - Monitor policy implementation and impact - Support regular review and resource allocation
Headteacher	- Lead a whole-school approach to online safety - Ensure robust safeguarding and reporting systems - Oversee staff training and parental engagement
Associate Headteacher Inclusion lead	- Support the Headteacher in implementing and monitoring online safety strategies - Lead on specific initiatives as delegated - Ensure online safety provision is accessible and differentiated for all pupils - Advise on inclusive resources and support
Computing Lead	- Coordinate the planning and delivery of the online safety curriculum - Provide staff training and up-to-date resources - Monitor curriculum progression and impact
All Staff	- Deliver online safety education as part of their teaching - Model safe and responsible online behaviour - Identify and report concerns promptly
Parents	- Reinforce online safety messages at home - Engage with school resources and workshops - Support children in safe use of technology - Participate actively in online safety education
Pupils	- Follow school rules for online behaviour - Report concerns and support peers

8. Inclusion

- Online safety education is differentiated to meet the diverse needs of all pupils, including those with SEND and EAL.
- Resources are adapted for accessibility, using visual supports, simplified language, and assistive technologies where appropriate.
- The Inclusion Lead works with class teachers to identify and address barriers to learning in online safety.
- Pupil voice is actively sought from all groups through circle time and digital leaders to ensure the curriculum reflects their experiences and needs.

9. Professional Development

- All staff receive regular, up-to-date training on online safety, including emerging risks and effective teaching strategies.
- CPD is provided through in-house sessions, external experts, and access to national resources.
- New staff receive online safety induction as part of safeguarding training.

10. Inspectorate Expectations

- This policy ensures a robust, whole-school approach to online safety, fully integrated into safeguarding and curriculum practice.
- Provision is age-appropriate, progressive, and responsive to current risks, with clear evidence of impact.
- Staff are trained, confident, and proactive in teaching and modelling online safety.
- Pupil voice is embedded in curriculum development and evaluation.
- Parental engagement is prioritised to extend online safety beyond the school environment.
- Monitoring, reporting, and review systems are in place and regularly evaluated for effectiveness.

11. Monitoring and Review

- The Computing Lead, in collaboration with the Headteacher and Governors, monitors the implementation and impact of this policy.
- Online safety incidents are recorded, analysed, and used to inform ongoing improvement.
- The policy is reviewed bi-annually, or sooner if required by changes in legislation or emerging risks.

12. Links to Other Policies

- Safeguarding and Child Protection Policy
- Computing Policy
- PSHE and RSE Policy
- Behaviour Policy
- Anti-Bullying Policy
- Equality and Inclusion Policy
- Data Protection and Privacy Policy
- Staff Code of Conduct
- Acceptable Use Policy (AUP)

Policy Review Sheet

Please note any comments or suggested amendments on this sheet. You may also choose to complete your comments in confidence on a separate piece of paper. Please add your initial to any comments.