Online Safety Policy

Approved by Governors Date: STILL TO BE RATIFIED
Review date: September 2026

1. Introduction

This policy sets out how Phoenix Primary School promotes safe, responsible and effective use of digital technologies. It supports the safeguarding of pupils and staff in line with the statutory requirements of Keeping Children Safe in Education (KCSIE), the UK GDPR, the Equality Act and the school's Safeguarding and Child Protection Policy. Online safety covers the use of the internet, digital communication, mobile devices, social media, gaming, remote learning platforms and all electronic technologies used in school.

2. Aims

The aims of this policy are to ensure that: pupils learn how to stay safe online and use technology responsibly; staff use technology safely and model appropriate behaviour; access to harmful or inappropriate content is minimised; incidents are reported and managed effectively; pupils are protected from online risks including grooming, radicalisation, bullying, exploitation and exposure to harmful content; school systems are secure and compliant with data protection legislation; and the curriculum supports pupils to develop critical awareness, digital resilience and understanding of online behaviour.

3. Roles and Responsibilities

The Governing Body ensures the school complies with statutory safeguarding requirements and monitors the effectiveness of online safety measures. The Headteacher ensures online safety is embedded across safeguarding, curriculum and staff training. The Online Safety Lead (often the Computing Lead or DSL) oversees monitoring, incident reporting and curriculum planning. The Designated Safeguarding Lead (DSL) leads on responding to online safety concerns, including liaising with parents, police or external agencies. Teachers deliver online safety education as part of Computing, PSHE and wider curriculum learning. All staff must read and follow this policy, the Safeguarding Policy, Staff Code of Conduct and Acceptable Use Policy (AUP). Pupils are expected to follow age-appropriate rules explained by staff. Parents are encouraged to support safe online behaviour at home.

4. Online Safety Education

Pupils receive regular online safety lessons through Computing, PSHE, the Jigsaw curriculum, assemblies, and themed events such as Safer Internet Day and Anti-Bullying Week. Online safety is embedded throughout our Computing curriculum using Kapow, and Phoenix Primary has adopted Option 2, which enables online safety themes to be revisited in every Kapow unit rather than taught as a single stand-alone block. This ensures regular reinforcement of key messages and supports progression across the school.

Teaching is age-appropriate, progressive across year groups, and adapted for pupils with SEND and EAL. Online safety education includes: keeping personal information safe; recognising unsafe or inappropriate online behaviour; responding to cyberbullying; understanding online friendships and digital footprints; safe use of gaming platforms; reporting concerns; and recognising misinformation. KS2 pupils also learn about grooming, scams, online challenges, exploitation and social media pressures. Jigsaw lessons reinforce respectful relationships, consent, managing feelings and staying safe online. Pupils are encouraged to speak to trusted adults whenever they feel unsure or worried.

5. Filtering and Monitoring

Phoenix Primary uses Trustnet (LGfL) Local Authority–approved filtering and monitoring systems to provide a safe online environment and minimise exposure to harmful or inappropriate content. These systems meet the DfE Filtering and Monitoring Standards (2023) and ensure internet access is age-appropriate and closely supervised. Internet activity may be monitored to identify safeguarding concerns or attempts to access restricted material. Any breaches or alerts are reported immediately to the DSL and recorded on CPOMS. Staff must not bypass or interfere with filtering systems. The school reviews filtering and monitoring effectiveness annually using the LGfL Online Safety Audit as part of our safeguarding evaluation.

6. Use of School Devices and Networks

Staff must use school devices for professional purposes only and follow the Staff Acceptable Use Policy. Pupils use school devices under supervision and follow the Pupil AUP. Personal devices may not be used to photograph or record pupils. Staff must use school email accounts for professional communication. All data must be stored securely and password protected.

7. Remote Learning and Digital Platforms

Where remote learning is used, it must follow safeguarding expectations. Staff should use approved platforms only, maintain professional boundaries, and follow the same behaviour expectations as face-to-face teaching. Pupils must not communicate with staff using personal devices or personal accounts.

8. Social Media

Staff must not communicate with pupils or parents via personal social media accounts. Staff should ensure their privacy settings are secure and maintain professional conduct at all times. Pupils are taught about safe and responsible use of social media, even if they are below the legal age for certain platforms. Any online reputation concerns or inappropriate posts involving the school must be reported to the Headteacher.

9. Cyberbullying

Cyberbullying is treated as a serious behavioural and safeguarding issue. Incidents involving threats, harassment, posting inappropriate images or sharing harmful content will be investigated following the Behaviour Policy and Safeguarding Policy. Consequences may include parental meetings, restricted access to devices, or referrals to external agencies.

10. Managing Online Safety Incidents

All online safety concerns must be reported immediately to the DSL or Online Safety Lead. The school will record incidents, investigate as necessary, and involve parents. If illegal content or activity is suspected, the police or the Local Authority may be contacted. Concerns involving safeguarding, grooming or exploitation are reported through established safeguarding procedures.

11. Data Protection and Digital Security

The school complies with GDPR and the Data Protection Act. Personal data must be stored securely, encrypted where appropriate, and only accessed by authorised staff. Staff must not use personal email accounts or personal cloud storage for school data. Devices must be locked when unattended.

12. Use of Images and Videos

Photographs and videos of pupils are only taken using school-owned devices and used in line with parental consent. Images must not be stored on personal devices. Staff must follow the school's Photography and Images Procedure.

13. Working with Parents

Phoenix Primary supports parents in understanding online risks by sharing guidance through newsletters, workshops, website links and signposting to national resources. Parents are encouraged to monitor their child's device use, apply parental controls, and discuss online safety regularly.

14. Training

All staff receive annual online safety training as part of safeguarding requirements. Additional training is provided where needed, including for new technologies or emerging risks.

15. Monitoring and Review

The Online Safety Lead and DSL monitor online safety incidents, curriculum delivery, staff compliance and filtering performance. The policy is reviewed annually by the Headteacher and Governing Body.

Reviewed:
Next Review:
Approved by Governors: