Phoenix Arch School

Kind, Curious, Creative and Collaborative

E-Safety

2026/27

School	Phoenix Arch School
Policy owner	Headteacher / Designated Safeguarding Lead
DSL	Falu Mehta
Deputy DSLs	Lennie Sarkis and Luana Oancea
Approval	Governing Body – September 2026
Review date	September 2027, or sooner if statutory guidance changes

Contents

Purpose and scope
Online risks
Teaching and family support
LGfL filtering monitoring and supervision
Personal mobile phones and smart devices
Staff use and images
Recording of pupils by members of the public
Safeguarding and online incidents
References
Safeguarding concern form
Staff Acceptable Use Policy (attached)
Pupil Acceptable Use Policy (attached)

1 Purpose and scope

- Read alongside the Behaviour and Regulation Policy, Safeguarding and Child Protection Policy, Staff Handbook and Induction Guide, and the Mobile Phone and Smart Device Policy.
- Online safety is part of safeguarding. This policy follows Keeping Children Safe in Education 2026, including Part Two on online safety and Part Four on concerns about adults.

2 Online risks

- Content includes harmful or illegal material, misinformation, extremist material, self-harm content and AI-generated or manipulated sexual imagery.
- Contact includes grooming, exploitation, impersonation and unsafe interactions with people or AI applications.
- Conduct includes cyberbullying, coercion and sharing private or sexual images without consent.
- Commerce includes scams, gambling, pressure to buy and financial exploitation.

3 Teaching and family support

- Revisit E-Safety at the start of each half term through lessons and assemblies. Adapt teaching using visuals, modelling and AAC as appropriate.
- Offer parent and carer workshops on online safety, recreational screen time and how to report concerns.
- Follow the Brent PHONE Pledge (Protect, Help, Observe, Nurture and Educate). Use it to guide safe technology use, support families and review practice.
- Use screens purposefully and with supervision. Reduce recreational screen time with practical, sensory, play-based and outdoor activities. Keep agreed AAC, assistive and medical technology available.
- Families may describe persistent difficulty stopping recreational use as “screen addiction”. Describe what staff observe, such as distress at stopping or effects on sleep, play or learning. Discuss patterns and support with families and the SENCO.
- Use visual timers, now-and-next cues, processing time and an accessible alternative. Share approaches with families, including predictable screen-free routines at home.
- Teach privacy, respectful behaviour, safe use and how to get help through computing and assemblies. Pupils can report concerns to any trusted adult using speech, visuals or AAC.
- Pupils do not use generative AI tools directly. Teach about AI risks through accessible examples. Staff use only approved tools and protect pupil information.

4 LGfL filtering monitoring and supervision

- Use London Grid for Learning (LGfL) filtering and monitoring on school networks and school-managed devices. Filtering helps block harmful content. Monitoring helps staff identify and respond to concerns.
- Supervise pupils on approved devices and preview resources. Pupils must not use personal email or social media in school. Teach safe gaming and online contact using age-appropriate examples.
- Report harmful material, alerts or gaps in protection to the DSL or DDSL and Computing Co-ordinator. If a pupil may be at risk, report immediately and record on CPOMS.
- The responsible senior leader reviews effectiveness at least once each academic year with the DSL and IT support. Check internet-connected devices in all relevant locations, record checks and actions, consider pupils’ age, SEND and access needs and report to governors.
- Train staff at induction and provide updates. Review online risks annually, including Prevent risks. Explain relevant safeguards, approved sites and planned online interactions to families.

5 Personal mobile phones and smart devices

- Phoenix Arch is phone-free throughout lessons, transitions, breaks and lunchtime. The rule also applies to clubs and school visits.
- Only Year 6 pupils may bring a basic mobile phone for an assessed independent travel need, with prior written Headteacher approval. Travel phones must be basic models. Hand the phone in on arrival for secure storage and collect it at dismissal according to the agreed travel plan.
- Personal smartphones, smartwatches and other connected or recording devices stay at home unless individually authorised, risk assessed and recorded for an agreed support need. Protect access to approved AAC, assistive technology and medical monitoring.

- Follow the Mobile Phone and Smart Device Policy for agreed transport handovers and school storage.

6 Staff use and images

- Keep personal phones silent and locked in staff lockers or securely at reception. Keep them out of classrooms unless the Headteacher has agreed an individual exception. Use personal phones in the staffroom during breaks or outside school hours, away from pupils. Disable wearable notifications during pupil contact.
- Use approved school devices and channels for work and contact with families. Personal devices must never be used to photograph or record pupils or staff, store pupil information or contact pupils or families.
- Parents, carers and visitors must keep devices put away around pupils and must not photograph, film or audio-record school events. School recording must be planned and consent obtained, with Headteacher oversight and approved equipment. Consult the DSL or DDSL about additional safeguards.
- Use strong passwords and approved secure communication systems. Keep pupil data on authorised systems and encrypted school devices. Follow consent, access and retention arrangements for images and records.
- Read and follow the Staff Acceptable Use Policy. Keep personal contact details private and use only approved school accounts and resources.

7 Recording of pupils by members of the public

- If a member of the public appears to be deliberately recording pupils through windows, at the gate, during transport handovers or on a visit, supervise and reassure pupils and move them out of view where safe.
- Tell the DSL or DDSL immediately, alert the office or visit lead and record the incident and action on CPOMS. Call 999 if a child is in immediate danger.
- On school premises, ask the person to stop if safe. In public places, avoid confrontation. Never pursue them, take or inspect their device, or demand deletion.
- If footage appears online, note the link and seek DSL advice before copying or sharing. The DSL or DDSL assesses risk and decides whether to contact families, police or children's social care, or report online content.

8 Safeguarding and online incidents

- Stop exposure to harmful material where safe. Reassure the pupil and follow the Behaviour and Regulation Policy for proportionate support and responses to device misuse and cyberbullying.
- Families can raise concerns with the class team or speak directly to the DSL or DDSL, including about incidents outside school. Use the school complaints procedure for complaints.
- Tell the DSL or DDSL immediately about any safeguarding concern and record it promptly on CPOMS. Call 999 if a child is in immediate danger.
- Report concerns about an adult's conduct to the Headteacher under the managing allegations or low-level concerns procedure. Report concerns about the Headteacher to the Chair of Governors. Alert the DSL or DDSL to any risk to a pupil.
- Record what happened, who was involved, the pupil's account, actions and decisions. Use the pupil's usual communication system and allow processing time.
- Do not routinely browse pupil devices, demand account access or delete potential evidence. Any search, confiscation or examination must be lawful, proportionate, recorded and handled by authorised staff under DfE guidance.
- If nude or sexual images of a child may be involved, seek immediate DSL or DDSL advice. Do not view, copy, forward or print suspected images, or ask a pupil to show them. Preserve evidence as directed.

References

DfE statutory guidance on mobile phones in schools
Keeping Children Safe in Education 2026 (September edition)
DfE guidance on searching, screening and confiscation
DfE announcement on strengthened phone-free school guidance
Government guidance for families on reducing screen time for under-fives
Government call for evidence on screen use by children aged 5 to 16
DfE filtering and monitoring standard
Brent Council's PHONE Pledge letter to families

Safeguarding Concern

Report any safeguarding concern immediately to the designated safeguarding lead (DSL) or a deputy (DDSL) and record it promptly on CPOMS. Recording does not replace speaking directly to the DSL or DDSL. Report concerns about an adult's conduct directly to the Headteacher under the managing allegations or low-level concerns procedure. If the concern is about the Headteacher, report it to the Chair of Governors. Alert the DSL or DDSL immediately to any risk to a pupil.

Staff Acceptable Use Policy

All staff are responsible for reading, understanding and following the Staff Acceptable Use Policy. This applies to permanent, temporary, agency and supply staff. Staff should ask the Headteacher or Computing Co-ordinator if they need clarification. All staff are responsible for reading, understanding and following the Staff Acceptable Use Policy. This applies to permanent, temporary, agency and supply staff. Staff should ask the Headteacher or Computing Co-ordinator if they need clarification.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not give out to pupils my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and Managed Learning Environment (MLE) tools for communications related to my professional role.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites will be a disciplinary matter.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not use personal accounts for streaming services such as Netflix on school laptops or iPads.
- I will not install any hardware or software without permission of the computing co-ordinator.
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. **I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.**
- I will make my school laptop available for inspection if required.
- Images & videos of pupils and / or staff will only be taken using school equipment, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & videos will not be distributed outside the school network / MLE without the permission of the parent/ carer, member of staff or Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute and I will monitor who my online friends are.
- I will ensure the safety of my laptop when on and off the school premises.
- I will only take data off the school premises on the school laptop.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

Pupil Acceptable Use Policy

These rules apply when pupils use school devices, the school network or school accounts, including when learning away from school.

Our rules for using technology safely

- I use my school device when an adult says it is time. I use the apps, websites and accounts they have agreed. I ask before opening a new link, downloading anything or using a chat tool. I leave AI tools for staff to demonstrate.
- I use kind words and respect other people online. I use my own school account and keep my password private. I ask staff for help if I need to log in.
- I keep personal information private. I check with a trusted adult before sharing my name, address, location or photos online.
- I ask a member of staff before taking or sharing a photo, video or sound recording. I follow their instructions about permission and where it can be shared.
- If something worries me, someone is unkind or a stranger tries to contact me, I stop and tell a trusted adult. I can use speech, signs, pictures or my communication device. I can ask for help even if I clicked something by mistake.
- I handle devices carefully and follow my class routine for breaks and putting equipment away. I can keep using my agreed communication aid, assistive technology or medical device as set out in my plan.

How staff support pupils

- Model and practise these rules in lessons and assemblies at the start of each half term. Use clear language, visuals, demonstrations and the pupil's usual communication system.
- Supervise device use and respond calmly to mistakes. Follow the Behaviour and Regulation Policy for support. Report safeguarding concerns immediately to the DSL or DDSL and record them on CPOMS.