



Boundary Oak School

Mobile Phone and Images Policy

2026-2027

Applies to staff, volunteers, contractors, pupils (day and boarding), parents and visitors. Read alongside Safeguarding, Online Safety & Acceptable Use, Staff Code of Conduct, Data Protection, Privacy Notices, CCTV and Behaviour/Anti-Bullying policies.

**PERSON RESPONSIBLE FOR
THE LATEST REVISION**

SLT/DSL/GDPR Officer

LAST REVIEW

January 2026

LAST UPDATE

September 2026 – Year 7 and below Brick
phone only.

NEXT REVIEW

January 2028

INTRODUCTION AND AIMS

At Boundary Oak School, the welfare and well-being of our pupils is paramount. The aim of this policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones and other devices are effective communication tools. It is recognised that it is the enhanced functions of many mobile phones and other devices that cause the most concern, offering distractions and disruption to the working day, and which are most susceptible to misuse – including the taking and distribution of indecent images, exploitation, and bullying.

1) PURPOSE AND SCOPE

This policy sets clear expectations for the carrying and use of mobile phones and other portable electronic devices and for taking, storing and using images of pupils. It balances the legitimate benefits of technology with safeguarding, privacy and data protection duties. It applies to all users on site and on school activities: staff, trainees, volunteers, contractors, pupils (day and boarding), parents and visitors.

2) PRINCIPLES & RELATED POLICIES

- Pupil welfare and well-being are paramount; professional boundaries and safe practice are expected of all staff.
- Mobile devices must not disrupt learning or compromise safety; usage should be mindful, courteous, and appropriate to the school environment.
- Image-taking is governed by UK GDPR/Data Protection Act 2018 and aligned with Keeping Children Safe in Education (KCSIE) and NSPCC best practice.
- This policy should be read with Safeguarding, Online Safety & Acceptable Use, Staff Code of Conduct, Data Protection, Privacy Notices, CCTV, and Behaviour/Anti-bullying policies.

3) STAFF: PERSONAL MOBILES & WORK USE

- During contact time with children, staff should not make/receive personal calls or texts except where essential for work purposes or with prior approval from the Head.
- Support staff follow supervisor directions regarding phone use. Emergency contact is via the School Office, landlines or walkie-talkies. Where communication is otherwise impossible (e.g., fields/woods/astro), carry a phone for emergency/logistics only.



- Mobile phones should not be used in spaces where children are present unless for specific work purposes on approved apps (e.g., Authenticator, ChatPro, Teams, Google Classroom, iSAMS, SOCS). In EYFS, personal devices must not be used in the presence of pupils. This reflects the EYFS Statutory Framework requirement to safeguard children and prevent unauthorised use of personal devices in early years settings.
- Staff must secure access to any personal or work phone (strong passcode/biometrics).
- For photographs, approved capture is on school equipment (cameras, iPads, school phones) or using personal devices via the ChatPro/Teams app under school controls; personal devices must not be used in EYFS and elsewhere only with Head's explicit approval.
- Before any storage or publication, check the photo-consent list. ChatPro/Teams images are not stored on devices and access is logged; only authorised staff may download to secure school storage.
- When image capture is authorised: be clear on purpose, inform pupils, respect any pupil who does not wish to be photographed, avoid one-to-one photography, ensure a senior member of staff is aware of the activity, and be able to justify images created.
- Report any concerning use of mobile devices to the Head/DSL.

4) PUPILS (DAY PUPILS)

- Pupils may bring a mobile phone to school but must hand it in, turned off, at Reception on arrival and collect it at the end of the school day. The school day constitutes all time on site.
- Pupils in Year 7 and below are only permitted to bring a 'Brick' phone into school, which must still be left in Reception. Smart phones will not be allowed for Year 7 and below.
- Pupils are not permitted to carry or use mobile phones or smart watches during the school day.
- Phones are not permitted on trips unless the trip leader has granted express permission in advance.
- If a phone or smart watch is found in a pupil's possession, it will be confiscated and held securely until the end of the day following a conversation with the pupil and issue of a CBS as appropriate.
- Unauthorised use is a behaviour incident and will escalate for repeated infringements.
- Parents should contact children via the School Office; pupils needing to contact home should use a phone made available by staff.



5) PUPILS (BOARDERS)

Boarders may use mobile phones during designated Tech Time in the evenings and under loose supervision at weekends. Phones must never be taken into dormitories or upstairs. Boarding staff will balance phone time with other activities. Parents may request limits; staff will apply professional judgement.

- Phones are handed out and collected to/from the tech cupboard under a sign-out/sign-in log.
- Phones are not allowed during the school day or on trips; misuse attracts the same sanctions as for day pupils.
- All phones must be named and secured with a passcode.

6) Trips & Off-site Activities

- Staff may carry/use mobiles for appropriate, professional communication and safety. Photographs of pupils may only be taken in line with this policy (approved devices/ChatPro/Teams, consent checked).
- Parent contact during trips is via the School Office/iSAMS or authorised school phones—not personal staff phones—except in emergencies or where insufficient school phones are available (e.g., DofE expeditions). This reflects OEAP National Guidance expectations regarding staff communications, device use, and safeguarding on off-site activities.
- The use of school owned trip moblies is recommended for all trips to aid the documentation of the trip and also contact from both the school and parents if need be. These are booked out via the office.
- Parent volunteers must not contact other parents about trip matters and must not take photographs of children.

7) PARENTS, VISITORS, CONTRACTORS

Parents and visitors should use phones courteously and appropriately on site. At school events, parents may photograph or video their own child. Do not publish images online that include other children. Never photograph in private areas (changing rooms/backstage). The school may refuse or withdraw permission if guidelines are not followed.



8) SMART WATCHES / SMART DEVICES

- Staff: apply the same precautions as for mobile phones.
- Pupils: smart watches/devices are not allowed in school.

9) LOSS, THEFT OR DAMAGE

The school accepts no responsibility for phones/devices that are lost, damaged or stolen on school premises/transport, visits or trips, or while travelling to/from school. Confiscated phones are stored securely at the School Office until collection. Lost phones should be handed in to the School Office.

10) TAKING, STORING & USING IMAGES OF PUPILS

10.1 Lawful Basis, Consent & Opt-outs

- Images where a child can be identified are personal data. The school will process them lawfully, fairly and securely under UK GDPR/Data Protection Act 2018.
- Parents/carers (or pupils, where appropriate—typically from age 13) are informed how images will be used and offered clear opt-out routes; individual restrictions (e.g., no website/social media) will be respected.
- High-risk cases (e.g., protected addresses/court orders) will attract additional controls, potentially including no external sharing and careful framing to avoid identification. For high risk cases the DSL will keep a confidential log and update accordingly when court orders/restrictions are lifted.

10.2 Where Images Must Not Be Taken

- Private/sensitive areas: toilets, changing rooms, medical rooms, staff rooms—no exceptions.
- Sensitive situations: disciplinary incidents, injuries/medical events, or where a pupil is distressed—unless explicitly directed and risk-assessed by the DSL/Head for safeguarding record-keeping.
- Never photograph a pupil when alone one-to-one with a staff member.

10.3 Devices & Controls

- Preferred: school-issued devices and approved apps/platforms. Where a personal phone is used in approved circumstances (e.g., on a trip), images must be transferred



immediately to secure school storage and deleted from the personal device the same day.

- Do not allow auto-backup to personal cloud; share only via school channels; keep devices locked with strong passcodes/biometrics.

10.4 Safe Capture Checklist

- Check consent lists before photographing a class/event; exclude or obscure opt-out pupils.
- Ensure pupils are appropriately dressed; avoid images revealing personal addresses, timetables or identifiable routines.
- No live-streaming of pupils unless separately risk-assessed and authorised by SLT/DSL with explicit written parent communication.

10.5 Storage, Retention & External Sharing

- Store images only on school-managed systems (SharePoint/OneDrive) with role-based access.
- Retention: identification images are deleted when the child leaves; curriculum evidence follows the records schedule; promotional images are reviewed at least annually and removed when no longer needed and in line with active informed consent.
- External sharing (website, press, social media): verify consent; apply “images-without-names / names-without-images”, use neutral captions, avoid tagging locations, consider time-delayed posting; conduct periodic audits.
- Third parties (e.g., professional photographers, media): use reputable providers, ensure contracts and due diligence; visitors are accompanied on site.

10.6 Incident Response (Images)

- Report concerns or inappropriate sharing immediately to DSL/DPO.
- Remove content from platforms; assess risk; inform affected families where appropriate.
- Log incidents and review controls; update consent lists as needed.

10.7 Staff Training

All staff receive annual training on image safety, online sharing risks and this policy (part of KCSIE awareness).



11) SANCTIONS & SEARCHING

Phones/smart watches seen in pupil possession are confiscated under sections 91 and 94 of the Education and Inspections Act 2006. Repeated confiscations may require parent collection. Where there is reason to believe a device contains illicit content or has been used to commit an offence or cause harm, authorised staff (DSL/SLT) may search in line with DfE guidance on searching, screening and confiscation. Criminal conduct (e.g., sexting; threats; abusive communications; impersonation/fake accounts) will be referred to police or appropriate agencies.

12) DISSEMINATION & IMPLEMENTATION

This policy is shared with staff and volunteers at induction and made available to parents via the School Office and website.

