

Mobile Phones Online Safety and Photographs

Little Lanes Out of School Club | Policy

Version: October 2026 | Applies to staff, volunteers, children, parents and visitors

Our commitment

Little Lanes uses technology in ways that protect children, respect privacy and keep staff focused on care. This policy covers phones, tablets, computers, cameras, smartwatches and other devices that can connect, record or share. It applies to Club activities, work communications and images taken for the Club, including outside session times.

Management authorises devices and uses, checks arrangements and explains this policy at induction. The designated safeguarding lead (DSL) handles online safeguarding concerns. All staff must report problems promptly and follow the Staff Behaviour and Code of Conduct and Safeguarding policies.

Staff phones and wearable technology

Personal phones must normally be switched off and stored in the locked black phone box on top of the cupboard during sessions. Staff must not wear smartwatches, Fitbits or other smart wearable devices. A medically necessary device requires an individually agreed adjustment that protects privacy and safety.

Urgent personal calls may be made using the Club phone or a personal phone in an agreed child-free area, with permission from the session leader and supervision covered. The kitchen may be used when child-free; another space must be agreed before use. Staff must not enter an unapproved classroom or leave children unsupervised. A family emergency requiring a phone to remain to hand needs prior manager or deputy permission.

Megan may carry her phone for authorised Club work, including access to emergency contacts. Routine use must be in a child-free area with supervision maintained. In an emergency, staff may use an available phone immediately to call for help or access necessary information. Moving to another area must not delay emergency action or leave children unsupervised.

Authorised work access on a personal phone requires a passcode, approved accounts and protection from access by others. Do not download child records to personal galleries or personal cloud storage. This exception never permits personal photography or recording of children.

Club devices and accounts

Use only management-authorised equipment for Club activities, including the Club television, interactive board and Amazon Fire Kids tablets. Management must check ownership or permission to use the equipment, maintenance and security before use. Personal staff tablets must not be brought into use without these checks and explicit approval. Use the authorised Club laptop, phone and camera only for approved work purposes. A child's or staff member's agreed medical or assistive device is an individual exception, not general permission to use personal equipment.

Management must check suitable security, software updates, access controls and privacy settings before a device or service is used. Use secure passwords, multi-factor authentication where available and automatic screen locking. Keep accounts restricted to authorised users, remove access when it is no longer needed and store devices securely after use. Do not connect unapproved storage devices or install apps without permission.

Never use personal devices to photograph, film or audio-record children at the Club. Only an authorised Club device may be used, subject to the photograph rules in this policy. Staff must not use personal accounts to communicate privately with children.

Children's personal devices

We discourage children from bringing phones, tablets, smartwatches or similar devices. If brought, they must be switched off and handed to staff at the start of the session for storage in the blue phone box, kept securely and inaccessible to children. Staff will identify whose device it is, record receipt and return, and return it to the appropriate child or authorised collecting adult at departure.

Children must not use personal devices during the session to call, message, browse, photograph, film or record. If a child needs to contact a parent, staff will help through the Club's arrangements. Parents should contact the Club, rather than the child's device, during sessions.

Agree essential medical monitoring, communication or assistive technology with parents and management in advance and document it in the child's plan. Keep necessary functions available and restrict unrelated recording, communication and internet access where practicable. Do not remove an essential aid without a safe alternative.

Little Lanes will take reasonable care of devices handed to staff, but parents are encouraged to leave unnecessary valuables at home. Report any loss or damage promptly and record what happened. Staff must not demand passwords or search a child's messages, photographs or browsing history as routine discipline; refer a concern to the DSL.

Safe use of screens and the internet

Little Lanes occasionally uses a Club television, an interactive board and Amazon Fire Kids tablets for planned, age-appropriate activities. The interactive board and tablets are used offline, without an internet connection. The television may be used for films, movement activities such as Danny Go, and quizzes, including selected content on YouTube Kids.

Staff check programmes, apps, games and downloaded content before use, considering every child watching or participating. Offline use and YouTube Kids do not replace content checks or active supervision. Staff control searches and playback. Children must not access settings, personal accounts or purchases, or enable an internet connection.

A staff member must remain present and actively involved. Agree suitable activity lengths, support turn-taking and provide breaks. Balance screens with outdoor play, movement, conversation and other activities. Offer a supervised alternative for children who do not wish to participate.

Films are occasional planned activities, not routine background viewing. Consider their length and suitability for younger children. For EYFS children, have regard to current DfE guidance favouring short, purposeful sessions with adult involvement, and consider screen use across their wider day. A full film is not a short session; plan shorter participation or an alternative for younger children as appropriate. Medical and assistive technology needs are considered individually.

- Use checked, age-appropriate content without adverts. Disable autoplay and prevent access to unsuitable recommendations; if a service cannot be used safely, choose another source or activity.
- Avoid background screens and using screens as routine behaviour management. For younger children, choose calm, suitable content.
- Do not allow social media, live chat with strangers, livestreaming, unapproved online games or generative AI tools.
- Teach children to ask an adult first, keep personal details private, be kind online and tell a trusted adult about anything upsetting or confusing.

Before children use an internet connection, management must confirm appropriate filtering and monitoring arrangements, including who deals with alerts. If using the school network, obtain confirmation of the protections available during Club hours; do not assume school safeguards cover every Club device. Where safeguards cannot be confirmed, do not give children internet access. Use checked offline content or a screen-free activity instead. Filters support, but never replace, supervision.

Parents and visitors

Parents and visitors must not use phones or other recording devices in areas where Club children are present, and must not photograph, film or record children. Ask staff before taking an urgent call and move to an agreed child-free area. Management may agree necessary medical, accessibility or official work use, with safeguards and no unauthorised recording.

A parent may ask staff for a photograph of their child's activity. Staff will check permissions and may provide a hands-only or activity image through an authorised private message. The no-faces rule and other children's privacy still apply.

Photographs and private parent messages

Little Lanes does not take activity photographs showing children's faces. We normally photograph hands, artwork or activities and share appropriate images privately with parents through authorised Club communication channels. We do not publish children's images on Instagram, the Club website or other public channels.

Take only images needed for an agreed purpose using an authorised Club device. Prefer an activity or artwork without children where this meets the purpose. The same privacy rules apply to video and audio; these must not be used to get around the no-faces rule or identify a child through their voice.

Permissions recorded on iPAL

Parents record photo permissions on iPAL. Management must ensure the permission clearly covers the proposed private sharing; if the wording is unclear, obtain clarification before taking or sending an image. Check the current permission and any safeguarding restrictions every time. School permission is not permission for Little Lanes.

For optional activity photographs, obtain informed agreement from a person with parental responsibility and respect the child's wishes. Do not photograph a child who refuses or appears uncomfortable. Children must not miss activities because photographs are declined. Permission does not override this policy's no-faces or no-public-posting rules.

A hands-only image can still identify a child through clothing, a name, another person, the background or the accompanying message. Staff must still check privacy and permissions rather than assume an image is anonymous because no face appears.

Parents can change their iPAL preference or contact management to withdraw consent. Staff will stop the affected use and management will arrange removal from Club-controlled records where applicable. An image already sent to its intended parent may not be retrievable. Essential identification or safeguarding records are considered separately under the appropriate lawful basis and privacy notice; activity-photo preferences must not delay necessary safeguarding action.

Taking images safely

- Never use a personal phone, camera or wearable device to photograph or record children. Staff must not keep personal copies.
- Do not capture faces, name labels, registers, medical information or computer screens. Check mirrors, windows and background reflections.
- Never photograph toileting, changing, intimate care or a child in distress. Children must be appropriately dressed and their dignity protected.
- Do not photograph a child's injury on a personal device. Follow safeguarding procedures and obtain appropriate professional advice about any necessary evidential image.

Sending a private message

Only authorised staff may send images through approved Club accounts and secure communication channels. Check the recipient and the image before sending. Send it only to the intended parent or carer authorised to receive information about that child, respecting any recorded restrictions. Do not use group messages, personal social media accounts or personal cloud albums.

An image sent to one family should not identify another child. Choose a different image or securely crop out unrelated children and identifying details before sharing. Ask parents to keep activity images private and not repost images identifying other children. Staff must not forward Club images to their own personal accounts.

Management must approve the security and privacy arrangements of any messaging service before use. Do not upload identifiable images or confidential child records to unapproved AI tools. If Little Lanes later wishes to use children's images publicly, management must first review this policy, assess risks and obtain separate informed permission. Existing iPAL permission for private sharing is not permission for publicity.

Storage and deletion

Keep images in approved, access-controlled Club storage. Transfer securely from the camera where needed and delete unnecessary device copies after checking the transfer. Disable geolocation tagging and personal cloud syncing. Management must document retention periods by purpose, review images regularly and securely delete them when no longer needed. Explain retention and sharing to families in the privacy information.

If something goes wrong

Act promptly if a child encounters upsetting content, receives unwanted contact, reports online bullying, or a device or photograph is misused. Concerns outside the Club can still affect the child's safety and must be taken seriously.

- Reassure the child, stop their exposure to harmful content and maintain supervision. Listen without blame and record their account in their own words.
- Tell the DSL or manager promptly. Record the time, device or service involved, what was observed and action taken. Use the alternative safeguarding reporting route if the concern is about that person.
- Do not investigate a child's accounts, impersonate them, contact a suspected offender or circulate material to colleagues. Obtain safeguarding or police advice.
- Do not deliberately view, copy, screenshot, forward or delete suspected sexual images of children. Stop viewing, restrict access to the device where safe and seek prompt DSL or police advice about preserving evidence.
- Call 999 where there is immediate danger. Follow the Safeguarding Policy for referrals, allegations against adults and relevant notifications.

For an unauthorised photograph, ask the person to stop when safe, inform management and record the concern. Do not physically seize or search a device. Management will decide next steps, including a request to remove an ordinary unauthorised image, or police/safeguarding advice where preserving evidence is necessary.

Lost devices and personal data breaches

Report a missing device, compromised account, misdirected photograph or accidental disclosure to management immediately. Secure the account or device where possible, restrict further sharing and preserve relevant records. Management will assess the information affected, risk to children and families, containment and any required reporting or notification under the Data Protection Policy. Staff must not conceal a mistake or attempt to resolve a serious breach alone.

Responsibilities and review

Management will keep an up-to-date record of authorised devices, services, access arrangements and photo permissions. Check controls after changes or incidents and confirm who receives online safety alerts. Any new app, device or method of sharing must be assessed before use, including privacy, security, age suitability and safeguarding risks.

Staff will be briefed on this policy at induction and when it changes, with online safety included in safeguarding training. Families will receive clear information about the rules and any planned use of children's images. Breaches may lead to restrictions on device use or appropriate action under the Staff Disciplinary or Visitors policy; safeguarding action takes priority.

Approval and review

Adopted by: Little Lanes Out of School Club

Date approved: October 2026 Review date: October 2027

Signed: MG Name and role: Megan Garratt - Manager

Review within 12 months of adoption and sooner following an incident, new technology or a change in guidance. This revised policy replaces the Mobile Phone and Wearable Technology Policy dated 1 September 2026.

References and related policies

Read with Safeguarding, Staff Behaviour and Code of Conduct, Data Protection and Confidentiality, Visitors, Equalities Inclusion and SEND, and Behaviour Management policies. Based on the current EYFS framework and the guidance below.

GOV.UK: EYFS statutory framework for group and school-based providers (September 2026).

GOV.UK: Safeguarding children and protecting professionals in early years settings: online safety considerations.

DfE: help-for-early-years-providers.education.gov.uk/health-and-wellbeing/screen-use

ICO: Taking photographs: data protection advice for schools (also relevant to clubs).