



Where Little Lambs Learn and Play

Policies and Procedures

PP11 – Mobile Phone & Social Media Policy

V1.0

November 2025

Document History					
Version	Type	Review Date	Reviewer	Approval Date	Approver
0.0	Initial Draft	15/11/2025	Jack Rogers	-	-
1.0	Publication	-	-		

This document is reviewed annually or sooner if required by changes in law, statutory guidance, or operational needs. Any changes, amendments, alterations, or updates of this document will be reviewed and/or approved by the Nursery Manager and a company Director.

All members of staff will be required to read this document in its entirety within 2 weeks of publication and for new starters before working with children, with confirmation that it has been understood.

Inevitably, there will be some situations that arise which are not specifically covered within this document. In such situation, if practicable, the Nursery Manager or Deputy Manager should be consulted for further guidance or instruction.

Any queries arising from this document should be raised with the Nursery Manager or Deputy Manager in the first instance.

This document and its policies and procedures herein, are not intended to replace recognised, established industry or regulatory safety standards, principles, or protocols.

Suggestions for future changes, amendments, alterations, additions, or updates should be sent to the Nursery Manager or Deputy Manager.

Copies of this document are uncontrolled and may not be current. If in doubt, please consult the Nursery Manager or Deputy Manager.

Table of Contents

1.	INTRODUCTION AND AIMS	3
2.	LEGAL AND REGULATORY FRAMEWORK	3
3.	DEFINITIONS.....	3
4.	STAFF USE OF PERSONAL MOBILE PHONES & DEVICES	4
4.1	Device Searching for Safeguarding Reasons	4
5.	VISITORS, PARENTS & CONTRACTORS	4
6.	NURSERY-OWNED DEVICES & DIGITAL SYSTEMS	5
7.	PHOTOGRAPHY, VIDEO & IMAGE USE	5
8.	STAFF USE OF SOCIAL MEDIA.....	5
9.	NURSERY OFFICIAL SOCIAL MEDIA CHANNELS.....	5
10.	STUDENTS, VOLUNTEERS & AGENCY STAFF	6
11.	ONLINE SAFETY, DIGITAL SAFEGUARDING & PREVENT DUTY	6
12.	DEVICE SEARCHING, SEIZURE & ESCALATION PROCEDURES	6
13.	EVENTS, PERFORMANCES & SPECIAL OCCASIONS.....	6
14.	REPORTING CONCERNS	7
15.	BREACHES AND DISCIPLINARY ACTION	7
16.	TRAINING, AWARENESS & REVIEW	7
17.	POLICY COMMITMENT	7

1. Introduction and Aims

Little Lambs Nursery recognises the benefits and risks that mobile phones, smart devices and digital technology present in early years environments. Whilst technology plays a significant role in modern communication, it also introduces safeguarding, privacy, confidentiality, reputational and data protection risks that must be managed rigorously. This policy establishes clear expectations for the safe, responsible and professional use of personal mobile phones, nursery-owned digital devices and all forms of social media within the nursery environment and during off-site activities. It aims to protect children from harm, uphold professional boundaries, safeguard personal data, and ensure staff conduct remains beyond reproach.

This policy must be read alongside **PP01 – Safeguarding & Child Protection Policy**, **PP02 – Health & Safety Policy**, **PP02B – Medication Administration Policy**, **PP04 – Business & Operations Policy**, **PP05 – Curriculum & Child Development Policy**, and the nursery's **Data Protection & GDPR Policy**. Together, these create the digital safeguarding framework through which all staff, students, volunteers, visitors and contractors must operate.

2. Legal and Regulatory Framework

This policy is informed by the following legislation, statutory guidance and regulatory expectations:

- **Early Years Foundation Stage (EYFS) Statutory Framework 2025**, including digital safeguarding, online safety, and use of personal devices
- **Children Act 1989 and 2004**
- **Data Protection Act 2018 and UK GDPR**
- **Human Rights Act 1998** – Article 8 privacy rights, balanced with safeguarding necessity
- **Working Together to Safeguard Children (2018, updated guidance)**
- **Prevent Duty Guidance** – online radicalisation and extremism risks
- **ICO (Information Commissioner's Office) guidance** on photography, data processing and mobile device use
- **Local Safeguarding Children Partnership procedures**
- **Ofsted expectations for online safety and digital device management in early years settings**

Compliance with these frameworks is mandatory for all individuals on nursery premises or representing the nursery off-site.

3. Definitions

For the purposes of this policy:

- **Personal mobile device** refers to any privately owned phone, tablet, smart watch, camera, wearable device with a screen, or digital communication tool.
- **Nursery-owned device** refers to any phone, tablet, camera or digital equipment issued by the nursery for professional use.
- **Smart watch** refers to any wrist-worn device capable of calls, messaging, photography, audio recording or internet connectivity.
- **Medical wearable** refers to a health-related device without a screen or digital communication function (e.g., insulin pump controllers, health trackers without displays).
- **Social media** includes all public or private online platforms, including Facebook, Instagram, X/Twitter, TikTok, WhatsApp, Snapchat, YouTube, forums and blogs.
- **Digital safeguarding risk** refers to any online or device-related action that could cause harm, including exposure to inappropriate content, grooming, radicalisation, exploitation, data breaches, unlawful sharing of information, or reputational damage.

These definitions ensure clarity and consistency when applying this policy.

4. Staff Use of Personal Mobile Phones & Devices

Personal mobile phones and smart devices must not be carried or used by staff in any childcare area. Personal phones must be stored securely in the locked office on arrival and remain there until the end of the shift. Phones must be on silent. Staff are responsible for ensuring personal devices brought into the nursery contain no illegal, inappropriate, or unsafe content.

A personal mobile phone may only be carried by a staff member where the nursery mobile phone is broken or unavailable and only with explicit approval from the Nursery Manager or Nominated Individual. This exception must be recorded and reviewed daily.

Urgent personal calls must be routed through the nursery office. If a staff member is expecting an urgent personal call, their phone may be held by the Nursery Manager, who will alert them. Staff may take or make urgent calls only in the office or outside the building, never in childcare areas.

Staff must not use personal phones to photograph, record, or communicate about children, parents, staff or nursery matters at any time. Staff must not use smart watches or wearable devices with screens. Medical wearables without screens are permitted.

4.1 Device Searching for Safeguarding Reasons

Where there is a **reasonable safeguarding concern**, the Nursery Manager and Designated Safeguarding Lead may request to inspect a personal device.

Searches must always:

- Be conducted by **two senior staff members**
- Be **proportionate, necessary, and justified**
- Be fully **recorded and logged**
- Include the staff member signing an **acknowledgement form**

If inappropriate, illegal or harmful content is found, the nursery will make immediate referrals to:

- The **Local Authority Designated Officer (LADO)**
- The **police**, where applicable
- The **Disclosure and Barring Service (DBS)**, if required
- The nursery's **internal disciplinary procedures**, up to dismissal

No staff member may refuse a search where safeguarding concerns are present.

5. Visitors, Parents & Contractors

Parents, visitors and contractors are not permitted to use mobile phones in any childcare area. Signs are displayed at all entrances and throughout the nursery.

Parents must end phone calls before entering. Visitors and contractors must sign in and store their phones in the office or leave them in their vehicle. Contractors may not use phones in any area where children are present.

Photography, recording or live-streaming by parents or visitors is strictly prohibited unless explicitly authorised for an event under controlled conditions (see Section 13).

Any breach of these rules will result in the individual being asked to stop immediately, delete any images taken, and, where necessary, leave the premises. Persistent non-compliance may result in withdrawal of access or safeguarding referrals.

6. Nursery-Owned Devices & Digital Systems

Nursery-owned tablets and devices are used exclusively for professional tasks such as observations, communication during outings and parent communication via Famly and email. Staff must never use personal accounts or non-approved apps for nursery business.

All nursery devices are password-protected, encrypted, and monitored. Only authorised staff may use them. Devices must not be taken into toilets, changing areas or sleep rooms. Internet access is filtered and app installation is restricted; where this is not yet in place, the nursery will implement filtering as a mandatory technical control.

Photos and digital content must be transferred weekly to secure nursery storage systems and deleted from devices. All digital communication with parents occurs through **Famly** or **email**, in line with the nursery's GDPR and safeguarding procedures. Staff must never store children's images on personal devices or cloud accounts.

7. Photography, Video & Image Use

Photography is carried out solely on nursery-owned tablets or cameras, whether on-site or during outings. No personal device may ever be used to photograph or record a child.

Photos must always respect children's dignity, avoid potentially embarrassing situations, and never be taken in intimate care spaces, toilets, sleep rooms or during nappy changing.

Live-streaming is strictly prohibited under all circumstances.

Parental consent for identifiable images is obtained on admission and reviewed annually. Group photographs where children are **not individually identifiable** may be shared without individual consent. Images may be used for observations, displays and the Famly app, in line with consent permissions.

All images are stored securely, access is restricted to authorised staff, and retention is consistent with GDPR requirements.

8. Staff Use of Social Media

Staff must maintain strict professional boundaries online. They must not post, discuss or reference the nursery, its children, families, activities or internal matters on personal social media platforms. Staff must not share photographs of the nursery or its children in any context.

Staff must not accept friend requests from parents or carers, nor engage in private online discussions about nursery matters. Staff may engage in general community discussions online but must avoid extreme, inflammatory or harmful online behaviour that could bring the nursery into disrepute or lead to parent complaints.

Staff must not identify themselves as nursery employees when posting material that could compromise professionalism, conflict with safeguarding expectations, or impact the nursery's reputation.

9. Nursery Official Social Media Channels

Official social media accounts may be operated by the Manager, Deputy Manager and Room Leads. Directors may grant additional access when required. All content must be authorised and reflect the values, professionalism and ethos of Little Lambs Nursery.

Account access must be protected through secure passwords and two-factor authentication wherever possible. Content sharing, including photographs, must comply fully with parental consent records. No staff member may store or edit nursery photographs on a personal device.

10. Students, Volunteers & Agency Staff

Students, volunteers and agency workers are subject to the same requirements as staff. Personal phones and smart watches must be stored in the office and not used during the day. Any breach of this policy will result in termination of placement or referral to the agency or training provider.

11. Online Safety, Digital Safeguarding & Prevent Duty

The nursery recognises that online safety is integral to safeguarding. Staff must be alert to risks such as grooming, exploitation, bullying, radicalisation, extremism, harmful content and digital fraud. Personal device misuse, including inappropriate messaging, sharing of images or accessing unsafe online content, may place children at risk and will be treated as a safeguarding matter.

Staff must follow Prevent Duty expectations by reporting any concerns related to online radicalisation or extremist content to the Designated Safeguarding Lead immediately, who will escalate according to **PP01 Section 4**.

The nursery uses filtering, supervision and monitored systems to reduce risk and provides staff with regular training on digital safeguarding in accordance with EYFS 2025.

12. Device Searching, Seizure & Escalation Procedures

Where safeguarding concerns arise relating to digital conduct, the nursery may temporarily seize and search a personal device following strict, lawful procedures.

Searches must:

- Be authorised by the Manager or DSL
- Be conducted by **two senior staff members**
- Be proportionate and limited to relevant content
- Be fully documented
- Include staff signing an acknowledgement

Illegal images or content will be reported immediately to the police and LADO. Devices may not be wiped, altered or returned until external authorities confirm it is appropriate. Serious concerns may result in immediate suspension, disciplinary action, DBS referral and safeguarding escalation.

13. Events, Performances & Special Occasions

At nursery events, parents and families are not permitted to take photographs or videos, except with explicit permission and only of their own child in designated areas. The nursery will take photographs on nursery-owned devices, edit them where appropriate, and share copies with parents according to consent records.

Parents who breach these rules will be reminded of safeguarding requirements and asked to delete any images or recordings. Repeated breaches may result in restrictions on attendance at future events.

14. Reporting Concerns

All staff have a duty to report any concerns about mobile phone, device or social media use immediately to the Nursery Manager or Designated Safeguarding Lead. Reporting must follow the procedures set out in **PP01 Sections 4, 6 and 7**. Staff are protected by whistleblowing legislation and internal nursery procedures.

Concerns relating to visitors, parents or contractors must be escalated immediately to the Manager or DSL, who will decide on further action.

15. Breaches and Disciplinary Action

Breaches of this policy are taken extremely seriously. Depending on the severity and nature of the breach, actions may include:

- Verbal or written warnings
- Suspension pending investigation
- Disciplinary action up to dismissal
- Referral to the **LADO**
- Referral to the **police**
- Referral to the **Disclosure and Barring Service (DBS)**
- Withdrawal of access for parents or visitors

The nursery will always prioritise the safety of children in all cases.

16. Training, Awareness & Review

Staff receive training on the safe use of mobile phones, digital devices and social media at induction and through regular safeguarding updates. Annual refreshers ensure familiarity with current legislation, risks and expected practice. Staff must sign annually to confirm they have read and understood this policy.

The policy is reviewed annually or sooner in response to new legislation, incidents, technological developments or safeguarding concerns. Updated versions are made available to staff and parents.

17. Policy Commitment

Little Lambs Nursery is committed to maintaining a safe, professional and digitally secure environment where children's rights, privacy and welfare are fully protected. By following this policy, all staff, visitors and parents contribute to a culture of safeguarding, trust and high-quality early years practice.

ENDS