Lilly Brook Childcare Ltd
Technology, Social Networking, and Media Policy

Contents

Reviewed

This policy will be reviewed annually or sooner if legislation or best practice guidance

When	First Review	Approval
11/12/2015	J Lindow	T Wilson
03/01/2016	J Lindow	T Wilson
16/01/2017	J Lindow	T Wilson
19/09/2017	J Lindow	T Wilson
05/08/2018	J Lindow	T Wilson
25/04/2021	J Lindow	J Wilson
01-09-2023	J Lindow	T Wilson
28/08/2025	J Lindow	J Wilson
16/02/2026	JLindow	T Wilson

Technology, Social Networking and Media Policy

Commitment to Safeguarding

Lilly Brook Childcare Ltd is committed to safeguarding and promoting the welfare of children, young people and adults at all times. Everyone connected with the setting is expected to share this commitment.

Technology and social media play an important role in communication and learning. However, they also present risks to privacy, confidentiality and safety. This policy explains how we manage those risks responsibly.

Scope

This policy applies to:

- staff
- students
- volunteers
- agency workers
- parents and carers
- visitors

It covers conduct both inside and outside working hours where individuals or the setting could be identified.

Key Principles

We will:

- protect children from harm and online exploitation
- preserve confidentiality
- maintain professional boundaries
- act quickly when concerns arise
- work in partnership with parents
- follow national and local safeguarding expectations

Staff Personal Device Use ("Phone Jail")

National safeguarding reviews repeatedly identify personal devices as a source of data breaches.

Therefore:

- Personal phones must be placed in secure storage on arrival.
- Phones must be turned off
- Emergency calls can be directed to the setting phone.
- They are accessible only during breaks or outside working hours.
- Smart watches must not be used for communication or photography.
- Personal devices must never be used to photograph or record children.

Failure to follow this may result in disciplinary action.

Use of Setting Devices

- Only setting equipment may be used for photographs or video.
- Devices are for EYFS and operational purposes only.
- They must not be used in toilets or nappy changing areas unless authorised by the DSL for safeguarding reasons.
- Personal browsing or accounts are not permitted.

Management carries out regular audits of images and storage.

Use of Public Social Media Platforms

Lilly Brook uses social media to promote understanding of early education, share good practice and give families insight into learning opportunities.

Because these are public spaces, we apply enhanced safeguarding controls.

Official Accounts

The setting may operate accounts on:

- Instagram
- TikTok
- YouTube
- Wix

Only authorised senior staff may post.

Passwords are stored securely and changed routinely.

Purpose of Content

Posts may include:

- demonstrations of activities
- educational messages
- staff training materials
- promotion of the setting
- safeguarding or awareness information

Protection of Identity

To minimise risk:

- No child's face will ever be shown.
- Names or personal details will never be shared.
- Videos focus on hands, feet or anonymised engagement.
- Live streaming is not allowed.

If there is doubt, content is not published.

Consent

Parents sign consent for anonymised promotional use at registration.

Consent can be withdrawn at any time and will be respected immediately.

Management checks consent records before publication.

Filming & Approval Process

- Only setting devices are used.
- Personal phones are strictly prohibited.
- All content must be approved by management before upload.
- Management may edit or refuse any material.

Public Interaction & Comments

These platforms allow public responses. Therefore:

- comments are reviewed regularly
- identifying or offensive remarks will be removed
- individuals may be blocked where behaviour presents a safeguarding risk

Serious issues are passed to the DSL.

Staff Conduct Online

Staff, students and volunteers must:

- never share confidential information
- avoid comments that could damage the reputation of the setting
- keep personal profiles private
- not identify children or families
- not accept parents as social media contacts
- maintain professional boundaries even outside work

They must not repost or discuss setting content from personal accounts in a way that increases risk of identification.

Online safety forms part of induction and ongoing training.

Parental Use of Social Media

We value respectful partnership.

Parents are encouraged to raise concerns directly with management so they can be addressed properly and fairly.

Parents must not:

- contact staff through personal accounts
- identify or discuss other children
- engage in harassment or cyberbullying
- speculate about attendance of any child

Where behaviour threatens safety or dignity, access to communication routes may be restricted while the matter is reviewed.

High-Profile or Vulnerable Families

Additional discretion is required.

No one connected to the setting may identify, discuss or attempt online contact with such families.

Concerns are escalated immediately via safeguarding procedures.

Cyberbullying & Harassment

Threatening or abusive digital behaviour is taken seriously.

Responses may include:

- removal of access
- investigation
- referral to safeguarding partners or other agencies

Incident Response

Where an online concern arises:

1. The DSL is informed immediately.

2. The incident is recorded and risk assessed.
3. Support is offered to affected individuals.
4. Material should be removed as quickly as possible.
5. External agencies will be informed where statutory guidance requires.

Legal & Statutory Duties

We operate in accordance with safeguarding, data protection and child welfare law. Notifications will be made to authorities where required.

Breaches of Policy

Action will be proportionate and may include:

- advice or training
- restricted online access
- disciplinary procedures
- termination of placement or employment
- referral to safeguarding agencies

Reporting Concerns

DSL: Jenna Lindow
Email: lillybrookchildcare@outlook.com
Phone: 07518 103023

Local Safeguarding: Bromley Safeguarding Children Partnership
Address: Bromley Civic Centre, Churchill Court, 2 Westmoreland Road, Bromley, BR1 1AS, UK
Telephone: 020 8461 7816
Email: BSCP@bromley.gov.uk
Website: **https://www.bromleysafeguarding.org/**
For child protection concerns or to refer to the Multi-Agency Safeguarding Hub (MASH):
MASH Telephone: 020 8461 7373 / 020 8461 7379 / 020 8461 7026
MASH Email: mash@bromley.gov.uk
Out-of-Hours Duty Service: 0300 303 8671 (emergencies)

Regulator: Ofsted
Telephone (general enquiries): 0300 123 1231
Email (general enquiries): enquiries@ofsted.gov.uk

Data Protection Officer (DPO): informationrequest@ofsted.gov.uk

Helpline hours: 8 am – 6 pm, Monday to Friday

Data Protection: Information Commissioner's Office (ICO)
Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK
Telephone: 0303 123 1113 (general enquiries)
Email (casework / concerns): casework@ico.org.uk

Online contact form: Available via https://ico.org.uk/global/contact-us/email/