Oughtrington Pre-School, Oughtrington Community Centre,Oughtrington Crescent, Lymm, Cheshire, WA13 9JD (Telephone 07808 111 278/ 757155 )

Registered Charity Number 1038655

Oughtringtonpreschool@gmail.com

***'Supporting Children to Flourish, Respecting and Nurturing their Individuality and Developing Strengths in Preparations for their Unique Learning Journey.'***

Mobile Devices, Images & Social Media Policy

Statement of Intent

We safeguard children’s privacy and wellbeing while celebrating their learning. This policy explains how we use setting-owned devices (pre-school phone/iPad) to record learning, how we prohibit personal device use in child areas, and how we manage social media and online safety in line with the EYFS 2025, UK GDPR and our Safeguarding Policy.

Scope and Roles

Applies to all staff, students, volunteers, contractors, visitors and committee members.Supervisor/DSL: Mollie Linley • Deputy DSL: Jemma Walsh • Data Protection Lead: Mollie Linley.

Personal Mobile Devices (including smart watches)

• Staff/visitors must store personal phones/smart watches in the designated lockable storage. They are not used in rooms accessed by children or during sessions except in an emergency and with Supervisor agreement.• No personal device may be used to take photos, video or audio of children or staff, on or off the premises.• Contractors/visitors are reminded of this policy on arrival; where a device is essential for work, it must not be used to capture children.

Setting-Owned Devices (pre-school phone/iPad only – no standalone cameras)

• Only the pre-school phone/iPad are used for photos, videos and observations (e.g., Tapestry/learning journal). No standalone cameras are used.• Devices are passcode-protected, encrypted, set to auto-lock and held under Supervisor control.• No personal accounts (Apple ID/Google) are signed in. Auto-backups to iCloud/Google Photos are disabled; AirDrop/Bluetooth file sharing is off.• Images are uploaded to approved platforms (e.g., Tapestry/secure server) the same day and then deleted from the device.• An audit log of access/use is maintained; misuse is investigated under Safeguarding/Disciplinary procedures.

Consent and Use of Images

• Written parental consent is obtained at registration and reviewed annually. We respect individual restrictions (e.g., internal evidence only, no social media, no group photos).• Children are not named in public posts; surnames are never used. We avoid sharing sensitive context (e.g., medical, safeguarding).• Consent can be withdrawn at any time and will be acted on immediately.

Storage, Retention and Security

• Images/recordings are stored within approved systems in the UK/adequate jurisdictions in line with UK GDPR and our Data Protection Policy.• Media is retained only as long as needed for educational records and then securely deleted.• Home working with images is not permitted unless expressly authorised and via secure systems.

Social Media (Closed Group)

• Our closed Facebook group is administered by the setting. Membership is limited to current parents, staff and committee; parents are removed when their child leaves.• No tagging, no surnames, no location sharing in real time. Posts use consent-checked images only. Comments are moderated and inappropriate content removed.• Parents’ own photos at events are for personal use only; if other children appear, publishing online should respect those families’ privacy.

Staff Personal Social Media and Messaging

• Staff do not ‘friend/follow’ current parents or discuss identifiable children online. No posting about the setting, children or colleagues.• No WhatsApp/DM groups with parents for operational matters; setting communication uses approved channels only.

Children’s E‑Safety and Online Learning

• Any child access to ICT is supervised. Content filters/safe search are enabled; apps and websites are pre‑checked by staff.• We promote early digital safety habits (asking a grown‑up, being kind online) appropriate to age/stage.

Breaches and Reporting

• Suspected misuse or a data/privacy breach is reported immediately to the Supervisor/DSL. Serious personal data breaches may be notified to the ICO within 72 hours and, if high risk, to affected families. Concerns about staff conduct may be referred to the LADO via safeguarding procedures.

Related Policies and Frameworks

Safeguarding and Child Protection • Data Protection/Privacy • Behaviour • Confidentiality • Complaints • Health & Safety • EYFS Statutory Framework (2025) • UK GDPR / DPA 2018

Review Statement

Updated September 2025. Reviewed annually or sooner if practice, platforms or legal guidance change.