Innsworth Preschool Technology, Media, and Screen Use Policy
Last Updated: 1st January 2026

1. Purpose and Scope

1.1 Overview: This policy defines the rules for the use of all technology, digital media, online platforms, and screens at Innsworth Preschool.

1.2 Objective: It clarifies our approach to media use, setting out the legal and operational boundaries for accommodating individual family preferences in a group care setting. The policy is designed to ensure our practice is safe, professional, and fully compliant with all statutory safeguarding, data protection, and confidentiality duties.

2. Legal and Statutory Framework

2.1 Compliance: This policy is reinforced by and compliant with our duties under the following legislation and guidance:

- The Statutory Framework for the Early Years Foundation Stage (EYFS).
- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- The Health and Safety at Work etc. Act 1974.
- The Equality Act 2010.
- Best Practice Principles: We draw on relevant principles (where applicable) from *Keeping Children Safe in Education (KCSIE)* and the Safer Recruitment Consortium's *Guidance for Safer Working Practice* to strengthen safer working practice.

2.2 Order of Precedence: If there is any conflict between policies: (1) Safeguarding and Child Protection Policy, (2) Data Protection Policy, (3) Parent-Provider Agreement, (4) this policy. Where a conflict relates to safeguarding risk, safeguarding controls prevail.

3. Core Principles

3.1 Approach:

- **Safeguarding First:** All use of technology and media is governed by our primary duty to safeguard children and protect their privacy.
- **Purposeful Use:** Technology is used in a limited way to support operations and enhance learning.
- **Professionalism:** We expect the highest standards of conduct from staff and parents in all online and offline communications.

4. Use of Technology by Staff and the Setting

4.1 Account and Device Management: All preschool-owned devices are for authorised educational and operational use only.

- **Information Security:** Any device storing children's data is encrypted and password-protected. We implement MFA where available, unique user accounts, least-privilege access, device lock timeouts, and regular patching.
- **Account Administration:** The Manager administers a joiners/leavers process to ensure prompt revocation of access. A device inventory is maintained by the Data Protection Lead.

- **Network:** Preschool internet access uses filtered internet and is restricted to professional use.

4.2 Artificial Intelligence (AI) Safeguard: Staff are strictly prohibited from entering any personal data, observations, or images of children into unapproved AI tools.

- **Definitions:** "Personal data" or "special category data" includes child names, health info, and photos. "Unapproved AI tools" are any AI/automation services not on our approved list and not covered by a written processor agreement and DPIA.
- **Authorisation:** Only the Manager (or nominated Data Protection Lead) may approve tools in writing. Approval requires a recorded DPIA decision, signed processor terms, and staff instruction.

4.3 Staff Personal Devices: In line with EYFS safeguarding requirements, staff are strictly prohibited from using personal mobile phones, cameras, or smart devices in any area where children are present.

- **Storage:** Personal devices must be switched to silent and stored securely in designated staff-only lockers.
- **Management Exception:** Emergency use only (calls/texts) is permitted for the Manager/Deputy. No browsing, messaging apps, photos, video, audio recording, or social media is allowed. Devices must remain out of children's reach and sight.

4.4 Data Incident Response: Any suspected data breach must be reported immediately to the Manager and Data Protection Lead. We assess reportability and, where required, notify the ICO without undue delay and within 72 hours of becoming aware, and notify affected individuals where required, in line with our **Data Protection Policy**.

5. Use of Technology by Children

5.1 Preschool Devices: Any device made available for children's use is strictly offline or uses a staff-supervised whitelist only.

- **Supervision:** Children's device use is always directly supervised (line-of-sight). A nominated staff member controls access. Accidental exposure is treated as a safeguarding incident and recorded per the **Safeguarding Policy**.

5.2 Smart Speakers: Innsworth Preschool does not use voice-activated smart devices (e.g., Alexa, Google Home) in child-access areas to protect privacy.

5.3 Children's Wearable Technology (Smartwatch Ban): Children are not permitted to wear smartwatches or connected devices with recording or tracking capabilities.

- **Handling:** We ask the parent to remove the device at drop-off. If discovered during a session, staff will ask the child to remove it; if the child will not, staff will disable functions where practicable (e.g., power off) and maintain supervision while the Manager contacts the parent. Secure storage is used if removal is achieved calmly.
- **Medical Exceptions:** Permitted only where supported by evidence (medical letter/plan) and a documented risk assessment. The plan specifies permitted functions, disables recording where possible, and outlines storage. The setting assumes "reasonable care" liability only.

6. Use of Media and Images

6.1 Consent, Capture, and Storage: We obtain prior written consent before taking or using any photographs or videos of children.

- **Withdrawal:** Consent may be withdrawn at any time and will not affect care; we apply the withdrawal from the point received.
- **Operations: I**mages are captured only on setting devices using approved apps (e.g., Tapestry). **I**mages are uploaded and deleted from the device promptly. No exporting to personal email or messaging apps is permitted.

6.2 Parental Sharing and AI Manipulation:

- **Sharing:** Parents must not post or forward any image/video containing other children. This breaches our privacy expectations and parent code of conduct and may trigger a placement review.
- **Deepfakes/AI:** Parents are strictly prohibited from using AI tools to alter, manipulate, or create "deepfake" images (e.g., face swap, voice cloning) using preschool photographs.
- **Enforcement:** Managed under the **Parent Partnership and Conduct Policy**; serious misuse (e.g., distribution or harassment) will be investigated and may be referred to the police/Local Authority.

7. Social Media and Professional Boundaries

7.1 Staff Boundaries: Staff are strictly prohibited from initiating or accepting 'friend' requests from parents of current children on personal accounts.

- **Pre-Existing Relationships:** These must be declared in writing to the Manager. Staff must not handle complaints, fee disputes, or safeguarding decisions involving families with whom they have a declared relationship.

7.2 Parent Conduct: Posting defamatory, hostile, or abusive content about the preschool, staff, or other families is a serious breach and may result in the termination of a child's place.

8. Curriculum and Educational Screen Use

8.1 Operational Limits: Screens are used for specific, time-limited purposes supporting the daily routine.

- **Duration:** Use is limited to no more than 20 minutes in any half-day session / 40 minutes in a full day (excluding emergency lockdowns or weather disruption).
- **Streaming Control:** Where streamed content is used, autoplay and recommendations are disabled; content is accessed only via pre-selected playlists in full-screen mode.
- **Rest Time:** Rest-time media is optional and used only for safe supervision and settling. Where practicable, we may offer a quiet activity area within the same supervised space for children who do not wish to view the screen.

9. Our Position on Parental Opt-Out Requests

9.1 Operational Necessity: By accepting a place, families acknowledge that occasional group screen use may occur as part of safe, supervised routines.

- **Supervision Rationale:** We cannot provide individual 'no screen exposure' guarantees without additional staffing that would compromise statutory ratios for the group.

10. Reasonable Adjustments (Equality Act 2010)

10.1 Process: Requests for adjustments must be in writing and supported by evidence. We assess via risk assessment and agree on a written plan with review dates. Preferences not linked to a protected characteristic may not be accommodated if they undermine ratios or group safety.

11. Breaches and Enforcement

11.1 Staff: Misconduct is managed under the **Disciplinary Procedure**; safeguarding-related misconduct follows the **Safeguarding Policy** and Allegations Management procedures, with LADO/Ofsted/Police/ICO referrals as required.

11.2 Parents: Breaches result in a formal review of the child's place. We may impose interim risk controls, such as restricting attendance at events or communication channels, while investigating.

12. Visitors and Contractors

12.1 Controls: Visitors/contractors must sign a no-recording declaration; refusal results in denial of access. Authorised device use is supervised and restricted to staff-only areas.

13. Training and Monitoring

13.1 Requirements: Induction, annual refreshes, and ad hoc updates follow changes. Staff sign acknowledgments, and training records are retained.