Innsworth Preschool Online Safety Policy
Last Updated: 1st January 2026

1. Purpose and Scope

1.1 Overview: This policy sets out Innsworth Preschool's approach to online safety, ensuring children are protected from potential harm from the online world.

1.2 Objective: Its purpose is to identify and mitigate online risks, provide a clear procedure for responding to any online safety incidents, and work in partnership with parents to promote a culture of digital safety.

2. Legal and Statutory Framework

2.1 Statutory Compliance: This policy is a core component of our safeguarding duties and is underpinned by the following statutory framework:

- The Statutory Framework for the Early Years Foundation Stage (EYFS) (Effective 1 September 2025): Specifically the safeguarding and welfare requirements regarding child protection and suitable people.
- Working Together to Safeguard Children.
- The Prevent Duty Guidance: Regarding the risk of radicalisation.
- UK GDPR and the Data Protection Act 2018.

2.2 Best Practice Guidance: We also have regard to relevant best-practice guidance, including:

- **Keeping Children Safe in Education (KCSIE):** We adopt relevant online safety principles from this guidance as best practice.

3. Roles and Responsibilities

3.1 Designated Safeguarding Lead (DSL): Has overall responsibility for online safety, including managing incidents, liaising with external agencies, and ensuring staff training is up-to-date.

3.2 All Staff: Are responsible for modelling safe online behaviour, strictly adhering to acceptable use rules, teaching children age-appropriate safety messages, supervising any use of technology, and reporting any concerns immediately to the DSL.

3.3 Parents and Carers: Are responsible for supervising their child's online activity at home and must adhere to our rules regarding the sharing of preschool data/images (e.g. Tapestry).

4. Identifying Online Risks

We distinguish between risks children may face in their home environment and risks managed within the setting.

4.1 Risks from Home Exposure (Parent-Controlled): Staff are trained to be aware of signs of harm resulting from:

- **Inappropriate Content:** Exposure to content that is sexual, violent, or age-inappropriate.
- **Online Bullying:** Negative online interactions between adults or siblings impacting the child.
- **Radicalisation:** Exposure to extremist content or ideologies via family devices.

4.2 Risks from Setting-Controlled Devices (Provider-Controlled):

- **Staff Misuse:** Unauthorised use of personal devices or social media.
- **Content:** Accidental exposure to unsuitable material via setting devices.
- **Data Breaches:** Accidental sharing of images or sensitive data (e.g. mis-posted Tapestry observation).

5. Protective Measures Within the Preschool

5.1 Technical Controls and Filtering:

- **Network:** Wi-Fi is password protected. The staff/business network is separated from any guest access.
- **Filtering:** Filtering is enabled at network/device level to block inappropriate content.
- **Video Content:** Content (e.g. educational videos) is pre-screened by staff. Autoplay and recommendations are disabled where possible. YouTube use is restricted to staff-selected content; "free browsing" by children is prohibited.

5.2 Supervision: All use of online materials by children is directly supervised by a staff member at all times.

5.3 Staff Acceptable Use Controls: To prevent abuse and protect data:

- **Setting Devices Only:** Staff must use setting-issued devices for observations/photos. Personal mobile phones/cameras are strictly prohibited for this purpose (see *Safeguarding Policy*).
- **No Personal Logins:** Staff must not use personal accounts (email, cloud storage) on setting devices.
- **Security:** Devices are protected by strong passwords/PINs and must be locked when not in use.
- **Prohibitions:** Downloading or screen-recording children's images onto personal devices is gross misconduct.

5.4 Age-Appropriate Education: We teach online safety in an embedded way using stories (e.g. "Smartie the Penguin") and discussions about "safe adults" and keeping personal information private.

6. Procedure for Responding to an Online Safety Incident

6.1 Definition: An online safety incident includes but is not limited to:

- A child disclosing something they have seen online.
- Staff concern about a child's welfare related to online activity.
- Data breaches (e.g. mis-sent message/photo).
- Unauthorised recording or sharing of images.
- Compromised accounts or lost devices.
- Online harassment of staff or families connected to the setting.

6.2 Response Protocol: In all cases, our main Safeguarding and Child Protection procedures will be followed:

1. **Immediate Action:** Secure the device/content if applicable. Listen calmly to the child (if a disclosure).
2. **Report:** Report immediately to the Designated Safeguarding Lead (DSL).
3. **Record:** The DSL records the date/time, nature of the incident, immediate actions, and outcome. Records are stored in the safeguarding file (restricted access) in line with retention schedules.
4. **Inform Parents:** The DSL will speak with parents to share the concern, **unless** doing so may increase risk to the child or prejudice an investigation (in line with our Safeguarding Policy).
5. **External Referral:**
    a. **Safeguarding:** If there is a risk of significant harm, refer to Children's Social Care/Police.
    b. **Radicalisation:** If signs suggest extremist influence, the DSL will seek advice via the Prevent channel.
    c. **Exploitation:** Specific online sexual exploitation concerns may be reported via CEOP/Thinkuknow.

7. Partnership with Parents and Data Safety

7.1 Tapestry and Digital Learning Journals: We use Tapestry to share observations securely.

- **Private Use Only:** Content is for personal family use only. Sharing images of other children (including in the background) on social media or group chats is a **breach of contract**.
- **Consequences:** Breaches may be managed under the Complaints, Code of Conduct, or Suspension & Termination policies depending on severity.

7.2 On-Site Recording: To protect all children, parents must not photograph or record video on site (e.g. at drop-off/collection) unless expressly authorised by management for a specific event.

7.3 Resources: We share trusted resources (e.g. NSPCC) to help parents manage online safety at home.

8. Training

8.1 Cadence:

- **Induction:** Online safety and acceptable use rules form part of the induction for all new staff.
- **Refresher:** Annual refresher training for all staff (or sooner if guidance changes).
- **DSL:** The DSL receives enhanced safeguarding updates consistent with the setting's training plan.

9. Monitoring and Review

9.1 Review: This policy is reviewed annually and immediately following any significant incident, or changes to the EYFS, safeguarding guidance, or data protection requirements.