

Innsworth Preschool Staff Safety, Site Security, and Lockdown Policy

Last Updated: June 2026

1. Purpose and Scope

1.1 Overview: This policy outlines the measures taken by Innsworth Preschool to ensure site security, manage intruder/lockdown/evacuation scenarios, protect staff safety, and maintain safeguarding during security incidents.

1.2 Hierarchy and Cross-Reference: This policy operates alongside our **Safeguarding and Child Protection Policy**, **Fire Safety & Evacuation Policy**, **Arrival/Departure Policy**, and **Critical Incident Plan**.

- **Precedence:** In any conflict regarding child welfare, the **Safeguarding Policy** prevails. In any conflict regarding fire egress, the **Fire Safety Policy** prevails unless an immediate external lethal threat exists (see section 7.4).

2. Legal and Statutory Framework

2.1 Compliance: This policy is informed by our duties under:

- The Health and Safety at Work etc. Act 1974.
- The Management of Health and Safety at Work Regulations 1999.
- The Statutory Framework for the Early Years Foundation Stage (EYFS).
- The Regulatory Reform (Fire Safety) Order 2005.
- The Equality Act 2010.
- ProtectUK / NaCTSO Guidance: We align with "Run, Hide, Tell" principles, adapted for the specific needs and ratios of an Early Years setting.

3. Core Principles

3.1 Approach:

- **Vigilance:** All staff must remain alert to their surroundings and report concerns immediately.

- **Prevention:** Robust physical security and strict access controls are our first line of defence.
- **Proportionate Response:** Actions must be calm, swift, and appropriate to the risk.
- **Life Safety:** The safety of children and staff is paramount. Our procedures prioritise gathering, accounting for, and supervising children over generic public guidelines.

4. Site Security and Access Control

4.1 Physical Security: All entry points and perimeter gates remain secured against external entry during operational hours.

- **Fire Egress:** Security measures must **never** impede emergency escape. Internal mechanisms allow for immediate exit without a key (e.g. thumb-turn locks or push bars), as validated in our Fire Risk Assessment.

4.2 Visitor Management:

- **Procedure:** All visitors (contractors, agency staff, professionals) must sign in, show photo ID where appropriate, and wear a visitor badge.
- **Supervision:** Visitors are **never** left unsupervised in child-access areas.
- **Deliveries:** Handled at the main door/gate; couriers are not permitted entry beyond the reception point.
- **Maintenance:** Essential maintenance during operational hours follows a strict "exception process" risk assessment to isolate the work area from children.

4.3 Challenging Strangers: Staff are empowered to challenge unfamiliar individuals, but only if safe to do so.

- **Protocol:** Use a polite, non-confrontational approach (e.g. "Can I help you?").
- **Safety:** Do not physically intervene. If a staff member feels threatened, they must withdraw to a safe area and escalate immediately: alert the Incident Lead, use the agreed code word, secure children, and call the police where necessary.

5. Incident Roles and Responsibilities

5.1 Command Structure: To ensure clarity during an incident, the following roles apply:

- **Incident Lead (Manager/Deputy):** Coordinates response, makes dynamic risk assessments (Lockdown vs. Evacuation), and issues instructions.
- **Police Liaison:** Communicates with 999 services.
- **Child Count Lead:** Ensures register is taken and all children are accounted for.
- **First Aid/Medication Lead:** Grabs the emergency bag (meds/first aid).
- **Cascade:** If the Manager is absent, the Deputy or most senior practitioner assumes the Lead role immediately.

6. Lone Working

6.1 General Rule: Lone working is generally prohibited. It requires prior written authorisation and is subject to a specific risk assessment.

6.2 Controls:

- **Permitted Tasks:** Low-risk admin, stock checks, cleaning (secure).
- **Prohibited Tasks:** Working with children (never permitted), cash handling, high-risk maintenance, or dealing with confrontational visitors.
- **Check-In Protocol:** Staff must check in with a named person on the **On-Call Contact Rota**.
- **Frequency:** Intervals are risk-based (e.g. on arrival, mid-task, on departure). Failure to check in triggers an immediate welfare check escalation.

7. Intruder and Emergency Response (Run, Hide, Tell)

7.1 Protocol: We follow "Run, Hide, Tell" adapted for Early Years. Child supervision and accounting for children take precedence over individual staff evasion.

7.2 Alerting Staff (Code Word): A discreet **Code Word** signals a threat without alarming children.

- **Security:** The code is stored in the staff handbook (not public policies) and shared during induction. Agency staff receive a briefing before deployment.
- **Change:** The code is changed only when necessary (e.g. staff changes or compromise).

7.3 RUN (Evacuation): If there is a safe route out, we evacuate.

- **Grab Bag:** Staff must take the emergency grab bag (register, contact numbers, first aid kit, essential medication/AAls, and the designated setting mobile).
- **Assembly:** Move to the fire assembly point or, if unsafe, across the street to the secondary off-site location on the embankment by the bridge.

7.4 HIDE (Lockdown): If evacuation is unsafe, we initiate **Lockdown**.

- **Action:** Move to designated lockdown rooms/areas. Lock doors/windows, close blinds, turn off lights.
- **Headcount:** Immediate register check. Keep children calm and quiet (e.g. read a story).
- **Fire Alarm Conflict:** If a fire alarm sounds during a lockdown, the Incident Lead conducts a **dynamic risk assessment**.
- *Rule:* If there is smoke/fire or instruction from services, **evacuate**. Do not delay evacuation unless police advise there is an immediate, lethal external threat at the exit route.

7.5 TELL (Communication):

- **Police:** Call 999 when safe.
- **Phones:** Only the designated setting emergency phone may be used. Staff personal phones must remain silent/stored to prevent noise, in line with our **Mobile Phone Policy**.
- **Blackout:** A strict communication blackout applies (no social media/parent calls) to prevent misinformation. This does not prevent calls to Emergency Services, the Local Authority, or statutory notifications.

8. Parental Conduct During Incidents

8.1 Access: During a lockdown or secure incident, doors will **not** be opened.

- **Procedure:** Parents arriving on site will be directed (via signage or central message, if safe) to a rendezvous point away from the danger area.
- **Primacy:** Police and Emergency Services take primacy on access control. Parents attempting to force entry risk compromising the safety of all children and will be managed under the **Parent Partnership and Conduct Policy**.

9. Equality and SEND

9.1 Adjustments: Emergency plans include reasonable adjustments for children and staff with disabilities or SEND (e.g. sensory needs, mobility issues). These are recorded in individual risk assessments or PEEPs (Personal Emergency Evacuation Plans) to ensure all children can be secured or evacuated safely.

10. Post-Incident and Records

10.1 Reporting: Following any security incident:

- **Debrief:** Full staff debrief and wellbeing support.
- **Notifications:** The Manager will assess reporting requirements to Ofsted (significant event), HSE (RIDDOR - if violence/injury occurred), and Insurers.
- **Learning:** Risk assessments will be updated.

10.2 Records: An **Incident Log** will be maintained (timeline, decisions, persons present, actions). Records are stored securely in line with GDPR and our **Data Retention Policy**.

11. Drills and Training

11.1 Governance:

- **Frequency:** Drills (Lockdown and Evacuation) are conducted at least termly.
- **Method:** Scenarios are varied (e.g. blocked route vs. intruder). Drills are age-appropriate and trauma-informed (e.g. "sleeping lions") to minimise anxiety.
- **Records:** All drills are logged with learning outcomes.

12. Enforcement

12.1 Proportionality: We distinguish between genuine errors under pressure (which require support/retraining) and reckless or deliberate breaches of security procedures (e.g. sharing codes, leaving gates propped open), which will be managed under the **Disciplinary Policy**.

