Confidentiality & Data Protection (GDPR) Policy (2025–2026)

Confidentiality and data protection (GDPR) Policy

1. Purpose

This policy sets out how Little Wonders Nursery ensures the confidentiality, integrity and proper protection of personal data (including children's, staff, parents/carers, visitors) in accordance with the UK GDPR (via the UK Data Protection Act 2018) and relevant ICO guidance, including in respect of CCTV/video-surveillance.

2. Scope

This policy applies to:

- All employees, volunteers, contractors and any other individuals working for or on behalf of the nursery.
- All personal data processed by the nursery: children's, parents', carers', staff's, visitors' and other third-party data.
- All physical, paper and electronic records, including CCTV/video-surveillance footage, images and audio recordings.
- All systems, premises and activities under the nursery's control where personal data or surveillance data is collected, stored, used or disclosed.

3. Legal / Regulatory Framework & Key Requirements

- The UK GDPR requires that personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date; stored no longer than necessary; and processed with appropriate security.
- The ICO has published specific guidance on video surveillance (including CCTV) for organisations, emphasising that surveillance must be **necessary and proportionate**, and that you must treat footage as personal data under UK GDPR.
- The Data (Use and Access) Act 2025 (DUAA) has received Royal Assent and will bring a range of reforms to data protection law. Organisations should already be

aware of upcoming changes (pending commencement) including new requirements for complaints handling, legitimate interests review, etc.
- The ICO in 2025 has published draft/enhanced guidance (for example on encryption) which may affect your data-security measures.
- For early years/child-care settings, the ICO also emphasises data protection obligations specifically for CCTV/footage and children's data.

4. Data Collection and Use

4.1 What we collect

We may collect personal data including, but not limited to:

- Children's names, date of birth, contact details (parents/ carers), emergency contacts, health/ medical information, dietary requirements, arrival/departure times, photographs/images (for registration and ongoing records).
- Staff and volunteer information: name, address, contact details, employment/contract details, training/qualifications, DBS checks, performance/HR records.
- Visitor/contractor records.
- CCTV/video-surveillance footage of children, staff, visitors (where applicable) for legitimate purposes (see 4.2).

4.2 Purposes of processing

We use personal data for operational, educational, safeguarding, health & safety, regulatory compliance and quality-improvement purposes. Specifically:

- To provide and monitor care and education of children.
- To communicate with parents/ carers and staff.
- To comply with our legal obligations (eg safeguarding, health & safety, regulatory inspections).
- To monitor and improve children's progress and wellbeing.
- Where we use CCTV/video-surveillance: to promote the safety and security of the premises, children, staff and visitors, to monitor access, deter and investigate incidents, and to support safeguarding.

4.3 Lawful basis for processing

We will identify and document the lawful basis for each processing activity (under UK GDPR). For example:

- Consent (especially for non-operational uses such as photographs for marketing or social media).
- Contractual or pre-contractual obligations (eg information needed for the childcare contract).
- Legal obligation (eg statutory safeguarding).
- Legitimate interests (eg CCTV for legitimate security/safeguarding interests) – ensuring a balancing test is documented and other rights are not overridden. The ICO emphasises legitimate interests must be carefully justified, especially in surveillance contexts.
- The DUAA may bring further changes to lawful basis / legitimate interests in due course; we will monitor and update accordingly.

4.4 Transparency and information to data subjects

We will provide clear privacy notices to children (where appropriate), parents/carers, staff and other individuals whose data we process. The notices will include: the identity of the data controller (the nursery), the purposes of processing, lawful basis, recipients/possible recipients, retention periods, rights of the individual (access, correction, erasure, etc), and specifically in relation to CCTV: where cameras are located, purpose of surveillance, retention period, contact for footage requests.
For CCTV where footage may be shared (eg with police) or accessed via subject access request, we will inform individuals of that possibility in our notices.

5. Consent and Access

5.1 Consent

Where we rely on consent (for example for use of children's photographs on social media or promotional materials), we will:

- Ensure consent is freely given, specific, informed and unambiguous (via clear affirmative action).

- Provide a mechanism for parents/carers (and where applicable children) to withdraw consent at any time, and inform them of the consequences of withdrawal (eg may affect marketing use but not necessarily care provision).
- Keep records of consent given.

5.2 Access, correction, erasure and other rights

Data subjects (or their authorised representatives) have the right to:

- Request access to the personal data we hold about them or their child ("Subject Access Request" / SAR).
- Request correction of inaccurate or incomplete data.
- Request erasure of data (in certain circumstances) or restriction of processing.
- Object to processing (in certain circumstances) and request portability (where applicable).
- In relation to CCTV/video-surveillance: individuals have a right to request access to footage of themselves. However, where footage also includes other people, we must consider the privacy of third parties; we may provide access after redaction or exclude third-party images. The ICO guidance emphasises this point.

We will respond to such requests promptly, in line with statutory timescales (within one month unless extended under law), and document our responses.

6. Data Security

6.1 Storage and access

- Electronic records: stored on secure servers or encrypted devices; access restricted to authorised personnel who need the data for their role. The ICO's 2025 draft guidance on encryption emphasises that encryption is a key security measure.
- Paper records: stored in locked cabinets/rooms, access restricted.
- CCTV footage: stored securely with access limited to designated authorised staff. Monitoring screens should be in secure areas only.
- We will ensure staff are trained in data protection principles, their responsibilities, and specifically how to handle surveillance footage, images and sensitive data appropriately.

6.2 CCTV / video-surveillance specific security

- We will ensure footage is protected from unauthorised access, alteration or deletion, stored for a defined retention period (see section 8) and encrypted or protected by access controls where appropriate.
- The cameras and recording systems must be managed with due regard to the necessity and proportionality of surveillance, with documented decision-making (see section 9).
- Audio recording via CCTV is only used when strictly justified; recording sound increases privacy risks and demands stronger justification.
- Where we outsource CCTV system/hosting/processing to a third-party, we will ensure a contract/data-processing agreement is in place specifying how footage is handled, stored, who has access, and how long it will be retained.

6.3 Breach management

- If a personal data breach (including unauthorised access/disclosure of CCTV footage) occurs, we will follow our incident/breach response procedures: containing the breach, assessing risk, notifying the ICO (if required) and affected individuals where necessary, and taking corrective action to mitigate further risk.
- We will document each breach, response and outcome.

7. Data Retention

- Personal data (electronic or paper) will be kept only for as long as necessary for the purpose(s) for which it was collected, and in accordance with any statutory retention requirements or guidance.
- CCTV/video-surveillance footage will be retained for a defined period (for example 30 days) unless required longer (eg for investigation of an incident, safeguarding/disciplinary, legal processes). The retention period must be justified, documented and reviewed periodically. The ICO emphasises that you should not retain footage longer than necessary.
- After the retention period elapses, data/footage will be securely deleted or overwritten, and paper records securely destroyed.
- We will maintain a retention schedule listing types of data, reasons for retention, and automatic deletion/archival processes.

Confidentiality and data protection (GDPR) Policy

8. CCTV / Video-Surveillance – Additional Specific Policy Items

8.1 Justification and proportionality

- Before installing or operating any CCTV/video-surveillance system, we will carry out a Data Protection Impact Assessment (DPIA) if the processing is likely to result in a high risk to the rights and freedoms of individuals (for example extensive coverage, children, audio capture, facial recognition, public areas). The ICO guidance states DPIAs are required for intrusive systems.
- We will ensure the system is justified by a legitimate purpose (for example safeguarding, child safety, crime prevention), ensure less intrusive alternatives have been considered, and that camera placement avoids unreasonable intrusion into privacy (for example avoid areas where children have a high privacy expectation, such as toilets/changing rooms).
- Any surveillance must be proportionate to the risks being addressed and must not be used as a default blanket monitoring tool.

8.2 Signage and transparency

- We will provide clear signage in all areas under surveillance indicating that CCTV is in operation, who operates it, the purpose of the monitoring, and contact details for enquiries/requests.
- Privacy notices will make reference to the surveillance system as part of our data processing activities.

8.3 Access, viewing and disclosure of footage

- Access to live monitoring and recorded footage is restricted to authorised staff who need access to perform their role (for safeguarding/security).
- If a request for footage is made (such as via a SAR) we will consider the rights and privacy of other individuals captured on the footage and may need to redact or blur third-party images or provide stills instead of full footage. The ICO emphasises this. ICO+1
- We will document requests for footage, our decision process and any disclosures.

- We will not use footage for any purpose other than for which it was collected (unless a new lawful basis applies) and will treat it as personal data.

8.4 Storage, review and deletion

- CCTV data will be stored securely and access logs maintained.
- We will regularly review camera coverage to ensure it remains necessary, appropriate and proportionate.
- Retention and deletion procedures for footage are set out in section 7.

8.5 Use of third-party/outsourcing

- If the CCTV system is managed, hosted or processed by a third party, we will ensure appropriate data-processing agreements are in place, that the third party is compliant with UK GDPR and ICO guidance, that footage storage is within a jurisdiction compliant with UK law, and that the third party's access, deletion and security procedures are documented.

8.6 Covert monitoring

- Covert surveillance (i.e., hidden cameras or secret monitoring) will **not** be used except in very limited circumstances (for example serious safeguarding investigations) and only where expressly justified, documented and proportionate – any use must be approved by senior management and comply with data-protection and safeguarding law.

9. Governance, Accountability & Training

- The Nursery Manager (or designated Data Protection Lead) is responsible for overseeing data protection compliance, including CCTV/video-surveillance.
- We will maintain a Record of Processing Activities (RoPA) covering all processing including surveillance, and ensure that any processing that is high risk has been assessed (via DPIA).
- We will review this policy at least annually (or earlier if law/guidance changes) and update our practices accordingly (including forthcoming DUAA changes).

- All staff will receive regular training in data-protection and confidentiality, including specific training on handling CCTV footage, children's data and subject-access requests.
- We will audit our data protection practices periodically, ensure compliance with ICO guidance and keep documentation (policies, decisions, risk-assessments, DPIAs, retention schedules, training records). The DfE/ICO audit closure summary emphasises the importance of governance and accountability (October 2023 update) in education settings.

10. Breach Notification

- We maintain an incident-response procedure. In the event of a personal-data breach (including unauthorised access, disclosure or loss of CCTV footage or other personal data), we will:
    - Immediately contain the breach, assess the nature and scope (which data, whose, how many, what harm).
    - Evaluate the risk to individuals and the organisation.
    - Notify the ICO without undue delay (and within 72 hours if feasible) if the breach is likely to result in a risk to individuals' rights and freedoms, and notify affected individuals if required.
    - Document the breach, the response, actions taken, mitigation measures and future improvements.
    - Review the incident to consider whether changes to policies, training or procedures are needed to prevent re-occurrence.

11. Review and Update of Policy

- This policy will be reviewed annually or sooner if required by changes in legislation, ICO guidance (including updates relating to DUAA), case law, or our operational circumstances.
- We will keep records of review dates, any changes made and version history.
- Staff will be informed of any changes to this policy and any significant changes will be communicated to parents/carers.

Confidentiality and data protection (GDPR) Policy

Appendix A: Key Definitions

- **Personal data**: information relating to an identified or identifiable living individual.
- **Processing**: any operation performed on personal data, including collection, recording, storage, use, disclosure, erasure.
- **Data Controller**: the organisation that determines the purposes and means of processing.
- **Data Processor**: a person/organisation processing personal data on behalf of a controller.
- **Video-surveillance / CCTV**: systems which record or monitor images (and possibly sound) of individuals, whether via fixed or mobile/temporary cameras, drones, body-worn or other forms of visual recording.
- **DPIA (Data Protection Impact Assessment)**: process to identify and mitigate the data-protection risks of a processing activity, particularly where that processing is likely to result in a high risk to individuals' rights.
- **Retention period**: how long a particular set of personal data (or footage) is kept before deletion or secure disposal.