Statement

At Twinkling Toddler, we prioritise confidentiality, privacy, and data protection. This policy complies with the revised Early Years Foundation Stage (EYFS, September 2025) and current General Data Protection Regulation (GDPR) guidelines, clearly outlining procedures for safeguarding personal data.

Confidentiality Commitments

- All personal information provided by parents and children is treated with strict confidentiality, upholding individuals' right to privacy.
- Staff members fully understand their confidentiality obligations, including potential consequences for breaches.
- Confidential information encompasses personal data, medical records, developmental observations, and other sensitive details.

To uphold confidentiality at all times, we will:

- Ensure that **parents/carers can access records relating to their own child only**. Information about other children will never be shared.
- Require that **staff do not discuss individual children or families** with anyone other than the child's own parents/carers, unless necessary and with prior consent.
- Keep **information shared by parents/carers confidential**, and only pass it on with their consent, unless a safeguarding concern overrides this.
- Ensure that **personnel matters** (e.g. staff performance, grievances) remain confidential to those directly involved.
- Store any **safeguarding concerns or evidence** in a secure, confidential file, accessible only to the child's key person, the Manager, and the Designated Safeguarding Lead (DSL).
- Comply fully with the **Data Protection Act 2018**, **General Data Protection Regulation (GDPR) 2018**, and guidance from the **Information Commissioner's Office (ICO)**.
- Ensure that any confidential information seen or heard by staff remains **within the nursery** and is not shared externally.
- Require that children's **abilities, behaviours, or needs** are only discussed with the child's parents or involved professionals, with parental consent—unless safeguarding concerns apply.

Storage and Access to Information

- Physical personal records are securely stored in locked cabinets accessible only by authorised staff.
- Electronic data is protected with robust passwords and industry-standard cybersecurity measures to prevent unauthorised access or breaches.
- Only authorised staff members have access to personal information necessary for their role.

Sharing of Information

- Personal data is shared solely on a **"need-to-know"** basis, always with explicit consent from parents/legal guardians.
- Data sharing with external professionals (e.g., healthcare or educational specialists) occurs only when necessary, appropriate, and with explicit parental consent.
- Written consent is obtained from parents for any photographic, video, or other media usage, clearly detailing purpose and duration of use.

Sharing Information in Exceptional Circumstances

- While we strive to maintain confidentiality, there may be **legal or safeguarding reasons** that require us to share information without consent.
- In such cases, information will be shared with relevant professionals on a **strictly need-to-know basis** and handled in a way that protects the welfare of the child and the integrity of all involved.

Data Protection

- Data processing adheres strictly to GDPR guidelines, ensuring data accuracy, relevance, and timely updates to meet childcare and legal requirements.
- Parents are transparently informed of data collection purposes, lawful processing bases, and their rights under GDPR, including rights to access, correct, or request deletion of data.

Data Breach

- Suspected or actual data breaches will trigger immediate internal investigation and prompt mitigation actions.
- Affected individuals and relevant data protection authorities are notified immediately as mandated by GDPR.

Retention and Disposal of Data

- Data retention aligns with GDPR principles, maintaining information only for as long as necessary for childcare provision and statutory requirements.
- Secure disposal methods (shredding physical documents or permanent deletion of electronic files) are rigorously employed when data is no longer required.

Staff Training and Awareness

- Staff receive regular GDPR and confidentiality training, clearly understanding responsibilities and required practices.
- All staff sign confidentiality agreements, formally committing to uphold privacy and data security standards.

Policy Monitoring and Review

The policy undergoes **annual** reviews, or more frequently if required, to maintain alignment with EYFS and GDPR updates.