GEMS TINEY HOME NURSERY

HOME FROM HOME CHILDCARE

Confidentiality and Data Protection Policy

Policy statement

At Gems tiney Home Nursery, we respect children's and families' privacy and handle personal information carefully. This policy explains how we collect, use, store, share and dispose of information in accordance with the UK GDPR, the Data Protection Act 2018 as amended, and current EYFS requirements.

Gemma Bayley is responsible for data protection within the setting and is the contact for questions, requests or concerns. This policy is supported by our privacy information and retention arrangements. It applies to employed and volunteer assistants and anyone authorised to handle setting records.

Information and lawful use

We collect information needed to provide safe childcare, meet safeguarding and EYFS duties, manage contracts and payments, support learning and communicate with families. This may include identity and contact details, attendance, parental responsibility, health and allergy information, care plans, development records, photographs, incidents and safeguarding concerns.

We identify and document an appropriate lawful basis for each purpose, such as legal obligation, contract, legitimate interests where appropriate, or consent. Health and other special category information also requires an appropriate additional legal condition. We do not use consent as a blanket basis for all processing.

Our privacy information explains the purposes and lawful bases, who information may be shared with, retention arrangements and relevant rights. We keep information necessary, accurate and up to date, use it only for legitimate purposes, protect it appropriately and keep evidence of compliance. Gemma checks and maintains any required ICO registration and data protection fee.

Confidentiality and authorised access

Information is discussed privately and only with people who need it for their role. Employed and volunteer assistants may access relevant records needed for safe care, such as allergies, emergency contacts and care plans, but do not receive unrestricted access to all family information.

Staff and volunteers must not discuss identifiable children or families with other parents, friends or unauthorised people, including on social media. Confidentiality continues after a person leaves the setting. This does not prevent appropriate safeguarding reports, whistleblowing or lawful disclosures.

Security and storage

Paper records are kept securely, with locked storage where appropriate, and are not left where families, visitors or children can access them. Electronic records are protected by appropriate access controls, strong passwords, device locks and updates. Multi-factor authentication is used where available and appropriate.

We use approved systems, including the tiney app, and check recipient details before sending information. Devices, backups and records taken on outings are protected against loss and unauthorised access. Access is removed when no longer required.

We minimise unnecessary downloads, printing and duplication. Identifiable records or images are not uploaded to unapproved apps, public AI tools or personal accounts. Any proposed new service is assessed for security, lawful processing and contractual safeguards, including overseas transfers where applicable.

Sharing information

We share relevant, accurate information with tiney and authorised professionals where there is a lawful basis and it is necessary for care, learning, safeguarding or another legitimate purpose. We explain sharing to families wherever appropriate and seek consent when that is the correct basis.

Safeguarding information can be shared without consent when there is an appropriate lawful basis and additional conditions where needed. We do not delay necessary protective action because consent is unavailable or refused. Parents are not informed in advance if doing so could increase risk or compromise an investigation. Reasons and decisions are recorded.

Only the information needed is shared, using a suitably secure method. Tiney has its own privacy information explaining its processing; we follow the relevant arrangements without assuming the agency and setting have identical data protection responsibilities.

Photographs and recordings

Photographs and recordings are taken, stored and shared under our permissions and safeguarding arrangements. Internal learning records and external publicity are treated as separate purposes. Where consent is relied on, it is specific, informed and can be withdrawn for future use.

Children's dignity and preferences are respected. We do not publish identifiable images without the appropriate permission and lawful basis, or share another family's private information. Families are asked not to photograph or share other children without permission.

Access requests and other rights

Requests can be made verbally or in writing; a particular form or legal wording is not required. We record the request, verify identity and authority proportionately and respond without undue delay, normally within one calendar month. Any lawful extension or clarification process is handled under current ICO guidance, with the requester informed as required.

Individuals may have rights to information, access, correction, erasure, restriction, objection and portability depending on the processing. These rights are not absolute: a request to delete information does not override necessary legal retention or safeguarding duties.

Children have their own data protection rights. A parent's request on a child's behalf is considered in light of their authority, the child's understanding and best interests, relevant EYFS duties and applicable exemptions. We protect other people's information and consider any risk of harm before disclosing records.

Personal data breaches

A breach may include lost records, a message sent to the wrong person, unauthorised access, accidental deletion or disclosure. Staff and volunteers must tell Gemma immediately; an incident involving tiney's systems is also raised promptly through the appropriate agency route.

We contain the incident, preserve relevant evidence, assess the risk to individuals, record the facts and decisions, and take corrective action. Every personal data breach is recorded, including those not reported externally.

Where notification is required, the ICO is informed without undue delay and, where feasible, within 72 hours of becoming aware. Notification is not required if the breach is unlikely to risk individuals' rights and freedoms. Where the breach is likely to create a high risk, affected individuals are also informed without undue delay, subject to applicable legal exceptions. We do not wait for a full investigation before making a required initial report.

Retention and disposal

We follow a documented retention schedule based on the record type, legal duties, safeguarding needs, insurer requirements and current guidance. There is no single retention period for all accident, attendance or safeguarding records. Relevant records may need to be kept after a child leaves.

Records due for disposal are securely shredded or deleted, including duplicate copies and backups where appropriate. Disposal is paused where information is needed for an ongoing safeguarding matter, claim, complaint or legal requirement.

Concerns training and review

Please raise questions or concerns with Gemma through the setting's usual contact routes. We investigate data protection concerns promptly and explain our response. You may also contact tiney about its processing and raise concerns with the ICO at https://ico.org.uk/make-a-complaint/.

Gemma ensures staff and volunteers understand confidentiality, secure handling, information sharing and breach reporting. This policy is reviewed annually or sooner if legislation, ICO guidance, systems or setting arrangements change. References: current ICO UK GDPR guidance and the EYFS childminder framework.

Policy owner: Gemma Bayley
Reviewed: November 2026
Next review due: November 2027