GEMS TINEY HOME NURSERY

HOME FROM HOME CHILDCARE

Mobile Phone Camera and Photographs Policy

Purpose and everyday use

Phones are needed during the nursery day for the tiney app, photographs, attendance and care records, parent contact and emergencies. Approved phones, including personally owned phones authorised for nursery work, may therefore be available and used by Gemma and assistants. This policy sets safeguards for their use rather than requiring phones to be switched off or locked away all day.

Safe professional use

Use must be brief, purposeful and compatible with safe supervision. Adults put the phone down whenever a child needs attention and agree cover for a task requiring concentration. Records can be completed later if immediate entry would compromise care. Phones must not distract from close supervision at meals, near water, during travel or other higher-risk activity.

Devices are kept out of children's reach when not in use but accessible to adults for necessary work and emergency calls. Personal browsing, social media and non-urgent calls or messages are limited to breaks away from childcare responsibilities. Urgent personal contact is managed with safe cover.

Emergency calls may be made wherever needed while children remain supervised. Adults must not leave children alone merely to make a call in private. Connected watches, tablets, cameras and other imaging or sharing devices follow the same safeguarding expectations.

Approved phones and security

Gemma approves the devices and users allowed to access nursery accounts or take images. Personally owned devices used for work require a secure screen lock, current updates, appropriate account protection and controlled access. Family members or other unauthorised people must not be able to view nursery records or photographs.

Use individual authorised accounts and multifactor authentication where available; do not share passwords. Disable inappropriate lock-screen previews, automatic sharing to personal or family photo libraries and unapproved backups. Use secure approved storage and transfer routes.

On leaving the role or ending use of a device, nursery access is removed and records or images are securely removed from the device in line with retention and evidence-preservation requirements. Devices are not sold, loaned or disposed of with accessible nursery data.

Taking photos and videos

We take a proportionate number of images for agreed purposes such as secure parent updates or learning records. Adults check the child's comfort and wishes and stop if the child is distressed or does not want to be photographed. Photographs never take priority over interaction or supervision.

No photos or recordings are taken during nappy changing, toileting, undressing or other intimate care, or of a child in a humiliating or inappropriate situation. Phones are not used for app entry during intimate care; the entry is completed afterwards.

We use agreed photo permissions and explain the lawful basis for the records we keep. Consent choices distinguish secure parent sharing, displays and external publicity. Parents can withdraw consent for future consent-based use, without affecting the child's place. Necessary safeguarding records follow the appropriate lawful procedures.

Storage sharing and publication

Images and care information are shared through the tiney app or another authorised secure route. Check the recipient and other children visible before sending. Necessary local copies are kept secure and deleted once securely transferred and no longer required under the retention arrangements.

Children's images or identifiable information must not be posted on staff personal accounts, sent through unapproved messaging or uploaded to unapproved AI tools. Public nursery publicity requires separate specific parental consent and appropriate permission for every identifiable child. Avoid identifying locations or personal details that could create risk.

We do not assume that personal cloud storage or a social platform is appropriate merely because it has a password. Gemma reviews access, storage, backup and deletion arrangements and the privacy information supplied to families.

Parents visitors and events

Parents and visitors must not photograph or record other children at the setting without explicit agreement. Any event photography arrangements are explained in advance and must respect all families' permissions. Adults may be asked to stop recording and address an unauthorised image; any safeguarding risk is escalated appropriately.

Visitors' phone use must not disrupt safe handover or reveal confidential information. Contractors and other visitors are supervised and follow the same restrictions on photography and intimate care areas.

Loss breaches and review

Report a lost device, unauthorised access, incorrect recipient or image-sharing concern to Gemma immediately. We secure accounts, revoke access or use safe remote controls where appropriate, assess the risk and follow data breach and safeguarding procedures, seeking tiney support. Where legally required, the ICO is notified within 72 hours of awareness and affected people informed without undue delay if the risk is high.

Do not copy or forward suspected child sexual abuse images; protect children from access and seek police advice about evidence. Relevant adult allegations follow LADO and tiney procedures. Gemma provides induction and reviews this policy annually and after incidents or technology changes. References: current EYFS childminder framework; UK GDPR and Data Protection Act 2018; ICO personal data breach guidance; Department for Education early years online safety guidance.

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