GEMS TINEY HOME NURSERY

HOME FROM HOME CHILDCARE

Internet Safety Policy

Purpose

We protect children from online harm and use technology carefully at Gems tiney Home Nursery. This policy covers children's access, staff and visitor devices, images, secure records and responses to concerns. It supports our safeguarding and data protection policies and current government early years screen use guidance.

Limited purposeful screen use

We prioritise conversation, hands-on play, movement, outdoor experiences and sleep. Screens are not used routinely to occupy or calm children, manage behaviour or fill transitions. They are not left on in the background or used at meals or within an hour before sleep.

We avoid screen time for under-twos apart from exceptional circumstances such as an agreed video call with a parent. For ages two to five, national guidance advises no more than one hour across the whole day, less where possible; this is not an allowance to use at nursery in addition to home use. We discuss relevant screen use with families.

Any use is brief, planned for a clear learning purpose and shared with an engaged adult. We avoid children using AI tools or toys with built-in AI features in line with current guidance. Assistive technology needs are considered individually with families and relevant professionals.

Content and access controls

Children do not browse freely, message strangers, use public chat or access social media. Adults check websites, videos, apps and links before use and assess content,

advertising, purchases, data collection and access to other material. There is no general EYFS approval scheme for apps.

We use suitable filters and device restrictions, disable autoplay and purchases where possible and choose advert-free, age-appropriate content. Controls support adult supervision and cannot guarantee safety. Devices used with children must not expose records, messages, photographs or account settings.

Phones cameras and connected devices

All adults follow the setting's rules for phones, cameras, tablets, smart watches and devices with imaging or sharing functions. Personal use must not distract from supervision. Visitors and parents must not photograph or record other children or use devices during intimate care.

Approved business use, such as a brief care record or necessary parent call, must maintain safe supervision. Devices are not used to take images during toileting, nappy changing or other intimate care. Children's own connected devices are discouraged and any necessary exception agreed individually and risk assessed.

Children's images are kept to the minimum needed. Parent updates use approved secure methods. Public or promotional use requires specific parental consent and respect for the child's comfort and wishes; refusing publicity does not disadvantage a child.

Privacy and device security

We use secure accounts, strong individual passwords, access locks, current security updates and multifactor authentication where available. Access is limited to authorised adults. Devices and records are stored securely, and loss or unauthorised access is reported promptly to Gemma.

We explain the lawful basis for care records and other personal information in our privacy information. Consent for publicity is separate from lawful sharing needed for care, safeguarding or legal duties. We do not assume a platform is safe merely because it is marketed for education or described as compliant.

Children's personal or identifiable information and images must not be uploaded into unapproved AI tools, personal social media or other unapproved services. We follow retention and breach procedures under our Confidentiality and Data Protection Policy.

Teaching safe habits and working with families

We use simple messages about asking a trusted adult for help, stopping if something feels upsetting and treating others kindly. Children are reassured that they can tell us without being blamed. We share suitable advice with parents and listen to concerns about home or setting use.

Responding to an incident

Stop the child's access, reassure them and prevent further exposure. Record the facts, time, service and relevant non-illegal details. Do not ask the child to repeat distressing content or investigate independently. Inform Gemma as safeguarding lead and take action proportionate to the concern.

Suspected grooming, exploitation or abuse follows our safeguarding referral procedures, including police or children's social care; immediate danger requires 999. CEOP or the Internet Watch Foundation may be appropriate reporting routes. LADO is used for relevant allegations about adults working with children, not every content error.

Do not screenshot, copy, download or forward suspected child sexual abuse images. Secure the device from children and seek police advice about preserving evidence. Inform parents unless doing so could increase risk or prejudice enquiries. Assess any data breach and reporting duties separately.

Training and review

Assistants receive online safety guidance through induction and safeguarding support. Gemma reviews devices, access and practice and updates this policy annually or sooner after incidents or changes. References: current EYFS childminder framework; Department for Education Screen use and Internet safety guidance; UK Council for Internet Safety early years practitioner guidance; relevant ICO guidance.

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