



Online Safety, Mobile Phones and Digital Devices Policy

Date policy was adopted:	17 th July 2024
Date last reviewed:	27 th August 2026
Frequency of review:	Annually or as needed.
Approved by:	Miss Anderson DSL/Mrs Moore DDSL/Jenni Taylor DDSL

Purpose

The Duckling Nursery is committed to safeguarding and promoting the welfare of every child. Technology can support communication, administration and children's learning, but it can also create safeguarding, privacy and developmental risks. This policy brings together the Nursery's previous Online Safety Policy and Mobile Phone and Electronic Device Use Policy into one safeguarding policy for children, staff, students, volunteers, agency workers, visitors and parents/carers.

This policy forms part of the Nursery's safeguarding arrangements and should be read alongside the Safeguarding and Child Protection Policy, Staff Code of Conduct, Whistleblowing Policy, Data Protection/Privacy Policy and Acceptable Use arrangements.

2. Statutory and guidance framework

The Nursery will have regard to the statutory Early Years Foundation Stage (EYFS) framework for group and school-based providers applying from 1 September 2026, including the requirement for the safeguarding policy and procedures to cover the use of mobile phones, cameras and other electronic devices with imaging and sharing capabilities. From 1 September 2026 providers must also have regard to Department for Education guidance on children's screen use in early years settings.

The Nursery also has regard to relevant safeguarding, Prevent, data protection, online safety and cyber security guidance, including UK Council for Internet Safety guidance for early years settings.

3. Leadership and responsibility

The Designated Safeguarding Lead (DSL), Miss Anderson, has lead responsibility for safeguarding and child protection, including online safety. The Deputy Designated Safeguarding Leads (DDSLs) are Mrs Moore and Mrs Jenni Taylor. All concerns about a child, an adult's conduct, inappropriate technology use, images, online communication or possible abuse must be reported immediately to the DSL or a DDSL in accordance with the Safeguarding and Child Protection Policy. Concerns will be recorded accurately and promptly, assessed and actioned, and external agencies will be contacted without delay where required.

Where the DSL or a DDSL is unavailable, or a practitioner reasonably believes that referring a concern internally would cause an unsafe delay, this must not delay safeguarding action. Any practitioner may contact Children's Social Care and/or the Police directly where necessary to protect a child. Staff must never investigate suspected abuse themselves or promise confidentiality. Concerns about unsafe or poor safeguarding practice must be escalated in accordance with the Whistleblowing Policy. Concerns or allegations about an adult working or volunteering in the setting must be reported immediately to the Manager or Deputy Manager; where the concern relates to the Manager, it must be reported to the

Assistant Manager, who will seek guidance from the LADO in accordance with the Safeguarding and Child Protection Policy.

4. Online safety risks

The Nursery recognises four broad areas of online risk:

- Content – exposure to illegal, inappropriate, misleading, extremist, discriminatory, sexual, violent or otherwise harmful material.
- Contact – harmful interaction with other people, including grooming, exploitation, coercion, scams or inappropriate communication.
- Conduct – behaviour online that causes or increases harm, including bullying, sharing inappropriate material, unsafe image-taking or loss of professional boundaries.
- Commerce – risks such as advertising, scams, phishing, in-app purchases and other financial or data exploitation.

5. Children's screen use from 1 September 2026

The Nursery will take a precautionary, child-development-led approach to screens. Screen use will be limited, intentional, supervised and linked to a clear learning, communication or accessibility purpose. It will not replace responsive adult interaction, physical play, outdoor experiences, books, conversation, sleep or other developmentally important activities.

- For children aged 2 to 5, the Nursery will keep screen use well below the recommended daily maximum of one hour, recognising that children may also use screens at home.
- Children will not access screens alone. An educator will co-engage with children and use conversation, questioning and interaction to extend learning.
- Content will be checked before use and must be age appropriate, safe, slow-paced and suitable for the intended learning purpose.
- Screens will not be used routinely to occupy children.
- Screen-based assistive technology for children with SEND or communication needs will be considered individually and is not restricted by general screen-time limits where it is necessary for inclusion, communication or wellbeing

Screens are only used where they have a clear educational or developmental purpose and where they enhance, rather than replace, active play, social interaction and hands-on learning.

Examples may include:

- showing a short educational clip linked directly to children's current learning or interests;
- supporting physical development through movement activities, such as Cosmic Kids Yoga or similar age-appropriate programmes;
- playing music or musical videos to support singing, rhythm, movement and music sessions
- accessing other short, age-appropriate educational content where this supports a planned learning experience.

6. Nursery-owned devices and internet access

- Nursery devices, including Apple I pads , laptops and nursery mobile phone, are for authorised Nursery purposes only.
- Access to devices and networks will be password/passcode protected. Passwords must not be shared inappropriately or left where children or unauthorised people can access them.
- Nursery devices will be stored securely when not in use and access will be managed and monitored by management.
- Only management may authorise or install apps, software or services. Apps, websites, search results and digital tools must be checked before use with children.
- Appropriate filtering, privacy and security controls will be used on internet-connected devices. Children must always be directly supervised and supported when accessing internet-connected technology.
- Personal or sensitive information will only be stored, accessed and shared in accordance with the Nursery's data protection and security procedures.
- Nursery devices must not be used for unauthorised personal social media, private messaging, personal email or other personal activity.

7. Personal mobile phones, smart watches and electronic devices

Staff, students, volunteers and agency workers must not use personal mobile phones, cameras, tablets, or other personal devices with imaging, or sharing capabilities while working directly with children. Personal devices must be stored securely in the safe or nursery cupboard during working time. They may only be accessed during authorised breaks, away from children and in the designated staff area.

Smart watches and wearable devices

Staff may wear a smart watch or other wearable device while working, provided that the device does not have a camera or other image-capturing capability.

While working directly with children, smart watches must be used only as a watch/timekeeping device. Staff must not use or engage with their smart watch to:

- read, send or respond to messages or notifications;
- make or receive calls;
- access social media, email or other communication applications;
- record or play audio or video;
- access the internet; or
- undertake any other personal activity that may distract them from supervising and caring for children.

Notifications should be disabled or silenced during working time wherever possible. Staff remain responsible for ensuring that wearing a smart watch does not compromise children's safeguarding, privacy, confidentiality or the practitioner's ability to provide appropriate supervision.

Any smart watch or wearable device with a camera or image-capturing capability is not permitted to be worn while working with children and must be stored securely with personal mobile phones.

Any exception required for a disability, health, medical, emergency or other legitimate reason must be agreed in advance with the Manager and, where appropriate, supported by an individual risk assessment.

Outings

During outings, the Nursery-owned mobile phone will be the primary device used for Nursery-related communication.

For safeguarding and emergency purposes, designated senior members of staff may also carry and have access to their personal mobile phones during outings. This provides an additional means of communication so that emergency assistance can be obtained and the Nursery or parents/carers can be contacted where necessary to safeguard children.

Where a senior member of staff has access to their personal mobile phone during an outing:

- the phone must only be used where necessary for safeguarding, emergency or essential Nursery-related communication;
- it must not be used for personal calls, messages, social media or other personal purposes while supervising children;
- it must never be used to photograph, film or make audio recordings of children;
- it must be kept securely on the staff member's person and must never be accessible to children;
- its use must not distract the member of staff from the effective supervision of children; and
- confidentiality and data-protection requirements must be maintained at all times.
- The Nursery-owned device will remain the preferred method of communication. Access to personal mobile phones during outings is a specific safeguarding measure for designated senior staff and does not alter the Nursery's general restriction on personal mobile phone use while working directly with children.

Devices Required to Support a Child's Medical Needs

Where a mobile phone, smart phone or other electronic device is required to monitor, manage or respond to a child's medical condition, its use is permitted where this forms part of the child's agreed healthcare or medical arrangements. This may include, for example, a mobile phone or application used to monitor a child's diabetes or glucose levels.

Access to such a device will be limited to designated senior staff and/or key staff who are responsible for caring for and monitoring that child.

Where a device is being used for this purpose:

- it may be accessed whenever reasonably necessary to monitor or respond to the child's medical needs;
- staff must remain alert to any alarms, alerts or notifications relevant to the child's health and act in accordance with the child's agreed medical arrangements;
- the device must only be used for the authorised medical purpose while staff are responsible for children;
- it must not be used to photograph, film or record children unless specifically required as part of an agreed medical procedure;
- it must be kept secure and, where appropriate, remain with the designated member of staff so that medical information and alerts can be accessed promptly; and

- staff must maintain the child's privacy and confidentiality when accessing or viewing medical information.

A child's health and safety will always take priority. The Nursery's restrictions on personal electronic devices will not prevent designated staff from accessing technology where it is reasonably required to safely monitor or manage a child's medical condition.

Any such arrangement will be agreed with the Manager and the child's parents/carers and, where appropriate, reflected in the child's individual healthcare arrangements and risk assessment.

8. Photographs, video, audio and recordings

Only setting-authorized equipment may be used to photograph, film or record children for legitimate Nursery purposes. The designated Nursery mobile phone must not be used to take or store photographs, videos or audio recordings of children.

Images and recordings will only be created and used where there is a legitimate Nursery purpose and the Nursery has the appropriate parental permissions and data protection basis.

Images will be stored and shared via Tapestry. They must not be copied to staff personal devices, personal cloud storage, personal email or personal social media.

Children's wishes and feelings will be respected in an age-appropriate way; staff should not force a child to be photographed or recorded.

Management will carry out proportionate checks of Nursery devices and recording practices to ensure safeguarding and parental permissions are followed.

9. Tapestry and electronic learning records

The Nursery uses authorised devices to record appropriate observations and photographs directly to Tapestry learning journeys. Tapestry and any other approved platform must be used in accordance with Nursery permissions, access controls and data protection procedures. Staff must use professional accounts and authorised devices only. Access must be limited to those who need it for their role.

10. Parents, carers, children and visitors

Parents/carers and visitors are asked not to use mobile phones or other personal devices with imaging or sharing capabilities within Nursery areas. Calls must be taken outside the childcare area. Devices must never be left where children can access them.

Children must not bring or use personal smart devices, cameras, smart watches or other connected, imaging or recording devices in the setting unless an individual need has been agreed in advance with the Manager and is managed through an appropriate safeguarding risk assessment.

At Nursery events, photography or video by parents/carers will only be permitted where the Nursery has clearly explained the arrangements and safeguarding/privacy requirements. Images containing other children must not be posted or shared publicly or on social media without appropriate permission.

11. Professional communication and social media

- Staff communication with parents/carers about Nursery matters must take place through approved Nursery channels such as Nursery email, telephone or approved platforms.

- Staff must not use personal accounts or personal contact details to communicate about Nursery business, and must not accept or initiate social-media connections with current children or families where this would blur professional boundaries. Any unavoidable pre-existing relationship must be declared to the DSL/manager and managed appropriately.
- Staff must maintain professional standards online and must not post confidential information, images of children, discriminatory or harmful content, or material that could compromise safeguarding or professional boundaries.
- Any concerning online behaviour by a colleague must be reported through safeguarding/allegations procedures; if the response is inadequate, staff must use the Whistleblowing Policy.

12. Cyber security and data breaches

- Staff must use strong passwords/passcodes, screen locks and approved storage and backup arrangements, and must not share credentials.
- Suspicious emails, links, attachments, password-reset requests, unexpected invoices or other possible phishing attempts must not be opened or acted upon and must be reported to management.
- Any loss of a device, unauthorised access, accidental disclosure, suspected hacking or other personal-data breach must be reported immediately to the manager/data protection lead so that containment, recording and any required notification can take place.
- Suspicious emails may be forwarded to the National Cyber Security Centre reporting service at report@phishing.gov.uk.

13. Reporting harmful or illegal online content

Safeguarding concerns must be reported immediately to the DSL or DDSL. The absence of the DSL or DDSL must never delay action necessary to safeguard a child. Where a child is at immediate risk of significant harm, there is an immediate risk to life, or serious immediate danger, staff must contact the appropriate emergency services, including the Police on 999 where required, and then inform the DSL/DDSL as soon as practicable. Any practitioner may make a direct referral to Children's Social Care where necessary to protect a child. Concerns about the behaviour or suitability of an adult will follow the Nursery's allegations/LADO procedures. Suspected child sexual abuse imagery or illegal online content must not be downloaded, copied, forwarded or investigated by staff.

14. Training, monitoring and review

Online safety and the safe use of mobile phones, cameras and digital devices form part of safeguarding induction, supervision and ongoing staff development. All practitioners must understand that safeguarding concerns can arise online as well as offline; know how to recognise, record and report concerns; understand allegations and whistleblowing procedures; and demonstrate safe professional practice. Management will monitor implementation, device use, permissions and emerging risks. This policy will be reviewed at least annually and earlier where the EYFS or other statutory guidance changes, local safeguarding procedures change, an incident identifies a need for review, Ofsted or the Local Authority recommends changes, or safeguarding practice indicates that procedures should be strengthened.

15. Breaches of this policy

A breach of this policy will be taken seriously. Immediate action will be taken to safeguard children and secure devices or information where necessary. Depending on the circumstances, a breach may lead to safeguarding or LADO procedures, referral to statutory agencies, data-breach procedures and/or disciplinary action. Staff must report concerns about unsafe practice and may use the Nursery's Whistleblowing Policy where appropriate.

16. Key references

- Department for Education – Statutory framework for the Early Years Foundation Stage for group and school-based providers, applicable from 1 September 2026.
- Department for Education – Screen use guidance for early years settings (2026).
- UK Council for Internet Safety – Safeguarding children and protecting professionals in early years settings: online safety considerations.
- Working Together to Safeguard Children and relevant local safeguarding partnership procedures.
- Data Protection Act 2018 and UK GDPR; Prevent duty guidance; National Cyber Security Centre guidance.