14
Mobile Phones & Digital Devices Policy

1. Policy Statement

At Peques Anglo-Spanish Nursery Schools, the safety, wellbeing, and privacy of children are paramount. This policy sets out clear expectations for the use of mobile phones, personal devices, and nursery-owned digital devices to ensure safeguarding, data protection, and professional conduct at all times.

This policy applies to all staff, including agency and bank staff, students, volunteers, visitors, and contractors across both settings.

2. Statutory Framework and Guidance

This policy is informed by and operates in line with the following statutory framework and guidance:

- Working Together to Safeguard Children (March 2026)
- Statutory Framework for the Early Years Foundation Stage (EYFS)
- Keeping Children Safe in Education (September 2025)
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

3. Purpose

This policy sets out the rules and safeguards in place for the use of mobile phones, personal devices, and nursery-owned digital equipment across all Peques settings. It applies to all staff, students, volunteers, visitors, and contractors. It must be read alongside the Safeguarding Children Policy and Procedure, the Online E-Safety and Digital Safeguarding Policy, and the Artificial Intelligence (AI) Policy.

4. Scope

This policy covers:

- Personal mobile phones and internet-enabled devices belonging to staff, parents, visitors, and contractors
- Nursery-owned digital devices including staff iPads, children's viewing devices, and office-based systems
- The Peques Digital Platform and all AI tools accessed through nursery devices

5. Mobile Phones - Staff

5.1 General Rules

Personal mobile phones must not be brought into any children's areas.

On arrival, all staff must:

- Switch phones off
- Leave them in the designated secure area
- Sign phones in on the daily log, which is shredded at the end of each day

The Manager or Deputy:

- Checks phones are submitted each morning
- Re-checks compliance following staff breaks

5.2 Breaks

Staff may use personal phones only:

- In the staff room, or
- Outside the building

Phones must remain switched off until the staff member has fully exited the nursery or entered the staff room, as applicable. Phones must be returned to secure storage and signed back in before the staff member re-enters children's areas.

5.3 Emergencies

Staff should provide the nursery phone number for urgent contact. Where this is not possible:

- A senior member of staff may hold the phone securely in the office
- The staff member will be informed when contact is received

Managers hold a company mobile phone for operational purposes, kept separately in the office and used solely for nursery business. Head Office also operates a company number for broadcasting urgent messages to parents where required.

6. Mobile Phones - Parents, Visitors and Contractors

All parents, visitors, and maintenance workers must:

- Switch phones off
- Leave them in the Manager's office

Contractors requiring phone access for their work:

- May keep their phone
- Will be supervised at all times whilst on the premises

7. Special Events and Photography

During registration, parents and carers must agree not to share content on social media where children other than their own may appear. Any breach results in the immediate withdrawal of permission.

Only nursery-owned devices may be used to take photographs or videos. All images are used solely for nursery purposes and in line with data protection requirements.

8. Personal Mobile and Internet-Enabled Devices

Personal internet-enabled devices are not permitted during operating hours, including:

- Mobile phones
- Tablets
- Smartwatches with SIM cards
- Smartwatches with WiFi connectivity

- Any device capable of receiving data, messages, or accessing the internet

Smartwatches that count steps only, with no SIM card, no WiFi, no data connectivity, and no ability to receive messages or access the internet, may be worn. Any uncertainty about whether a device falls within this restriction must be referred to management before the device is brought into use.

9. Children's Access to Digital Devices

9.1 Purpose

Children do not use or handle nursery iPads or other digital devices. On occasion, children may watch pre-approved educational content on a nursery device as part of the EYFS curriculum to support learning and development. Any such use is always directly supervised by a member of staff.

9.2 Safeguards

Children do not have access to:

- The internet
- Cameras or video functions
- Data storage
- Messaging or communication features
- Independent handling or operation of devices

Any educational content shown to children must be approved in advance by management. Devices always remain under staff control and are stored securely when not in use.

9.3 Procedure

- Children are always directly supervised by staff
- Children do not independently operate or handle devices
- Educational content must be pre-approved by management
- Staff may suggest content for review; however, installation or access can only be authorised in line with nursery procedures
- Devices must remain under staff control at all times

10. Staff PCs and Office-Based Digital Systems

10.1 Purpose

Staff PCs and office-based digital systems are used only for authorised nursery business, including administration, record keeping, safeguarding, and communication. Children never have access to staff PCs, office computers, or office-based digital systems under any circumstances.

10.2 Security and Restrictions

Access to staff PCs and office-based digital systems is restricted to authorised staff only. Devices are password protected, physically secured, and used solely for authorised nursery business.

Internet access on company PCs is filtered and monitored. Peques uses Kaspersky Safe Kids on company PCs to strengthen internet filtering and restrict access to inappropriate or unauthorised websites.

All data accessed or stored through staff PCs and office-based digital systems is managed in line with safeguarding, confidentiality, and UK GDPR requirements. Any misuse of company PCs, unauthorised access, or attempt to bypass device restrictions may result in disciplinary action and will be managed in line with the Safeguarding Policy.

11. Staff iPads and Nursery Devices

11.1 Purpose

Staff devices are used only for:

- Observations and assessments
- Activity planning
- Approved communication
- Uploading learning updates via Famly, the sole authorised parent-facing platform

11.2 Security and Restrictions

All staff devices:

- Are managed centrally via secure device management software
- Have individual six-digit passcodes
- Automatically lock after one minute
- Remain on nursery premises in a locked room
- Have no iCloud accounts
- Have AirDrop disabled
- Cannot download or delete apps
- Cannot access social media or adult content
- Have restricted web access to approved sites only

Only designated Head Office staff can:

- Change settings
- Install or remove apps
- Adjust restrictions

11.3 Images and Media

Photographs and videos taken for nursery purposes must:

- Be taken only on approved nursery devices
- Be uploaded, stored, and shared only through approved nursery systems
- Not be retained on devices longer than necessary under nursery procedure
- Never be transferred to personal devices or personal accounts

Children must never use staff devices.

12. Acceptable Use of Nursery Digital Devices

12.1 Acceptable Use - Staff May

Staff may use nursery devices only for legitimate nursery purposes, including:

- Educational planning
- Observations and assessments

- Uploading learning updates to Famly
- Approved nursery communication
- Accessing the Peques Digital Platform for authorised staff support purposes, in line with the Artificial Intelligence (AI) Policy, Policy 7

Use must always be professional, purposeful, appropriate, and safeguarding-focused.

12.2 Unacceptable Use - Staff Must Not

Staff must not:

- Use devices for personal browsing or personal communication
- Access personal accounts or social media
- Download, delete, or modify apps
- Attempt to bypass restrictions
- Share files, images, or data externally
- Store children's images outside approved systems
- Allow children access to staff devices
- Use any external AI tool or internet-based AI service on any nursery device
- Use any personal AI application on a personal device during breaks or at any other time in connection with Peques business

The Peques Digital Platform is the only approved AI system for staff. All requirements are set out in the Artificial Intelligence (AI) Policy, Policy 7.

12.3 Monitoring and Accountability

Nursery device use may be monitored in line with nursery procedures, safeguarding responsibilities, and data protection requirements. Safeguarding overrides convenience at all times. Any breach of acceptable use expectations may result in disciplinary action, safeguarding review, or both.

13. Data Protection and Privacy

All digital use complies with UK GDPR and data protection legislation:

- Images must be shared only through approved nursery systems
- No images of children may be stored on personal devices
- Personal data must be accessed and processed only where necessary for legitimate nursery purposes
- Devices and records containing personal or safeguarding information must be kept secure at all times

Any data breach, suspected breach, loss of device, or unauthorised disclosure of information must be reported immediately in line with nursery procedures.

14. Breaches of Policy

Any concern relating to mobile phones, digital devices, unauthorised recording, inappropriate content, misuse of technology, data security, or possible online harm must be reported without delay.

Where the concern relates to child safety, staff conduct, images of children, inappropriate communication, or any other safeguarding matter, it must be managed in line with the Safeguarding Children Policy and Procedure.

Any breach of this policy may result in:

- Disciplinary action

- Internal investigation
- Safeguarding investigation
- Referral to external agencies where required

This policy should be read in conjunction with:

- Safeguarding Children Policy & Procedure
- Confidentiality & Information Sharing Policy
- Online E-Safety Policy
- Social Media & Networking Policy
- Artificial Intelligence (AI) Policy
- Company Code of Conduct Policy
- Peques Privacy Notice

Version: 1.1
Effective date: 20/03/2026
Last reviewed: 20/03/2026
Review cycle: Annually, or earlier where required due to legislative, regulatory, operational, or statutory changes.
Approval route: Head Office