13

Online E-Safety & Digital Safeguarding Policy

(Safe, Responsible and Purposeful Use of Technology at Peques)

1. Purpose and Scope

Peques is committed to safeguarding children from harm in both offline and online environments. We recognise that digital and online technologies form part of modern life and that children must be protected from exposure to inappropriate, harmful, or extremist content. This policy sets out our approach to safeguarding children, families, and staff from the risks associated with digital technology, online content, and internet access, and how Peques promotes and maintains online safety within the nursery in line with our wider safeguarding responsibilities.

This policy applies to all staff, including agency and bank staff, students, volunteers, visitors, contractors, and parents and carers across both Peques settings. It covers all digital devices, online platforms, and AI tools used on or in connection with Peques premises. Online safety is part of the nursery's wider safeguarding culture and must be understood and applied by all.

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) (September 2025)
- Keeping Children Safe in Education (September 2025)
- Counter-Terrorism and Security Act 2015 (Prevent Duty)
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Information Sharing: Advice for Practitioners (May 2024)
- ICO guidance on children's data and online privacy

3. Aims

- To protect children from inappropriate online content, unsuitable use of digital devices, and digital safeguarding risks
- To promote safe, responsible, and purposeful use of technology by staff, children, and families
- To ensure all digital tools and devices used at Peques are secure, controlled, and fit for purpose
- To embed a culture in which digital safety is understood as an integral part of safeguarding
- To ensure compliance with statutory safeguarding, data protection, and online safety legislation

4. Safeguarding and Online Safety

Peques takes active steps to ensure that effective procedures are in place to protect children from the unsuitable use of digital devices and from exposure to inappropriate material within the setting.

Online safety is embedded within the nursery's wider safeguarding approach. Concerns relating to online content, online contact, online conduct, or online exploitation must be treated as safeguarding concerns and responded to in line with the Safeguarding Children Policy and Procedure.

Peques recognises that online risks may arise through digital media used within the setting, family circumstances, home access to technology, wider community exposure, or the behaviour of adults. Staff must remain vigilant to signs that a

child may be affected by harmful online content, inappropriate contact, grooming, exploitation, coercion, or exposure to extremist material.

5. Use of Digital Devices in the Setting

- Only nursery-approved digital devices are used within the setting
- All digital devices are purchased new to reduce the risk of hidden, unauthorised, or inappropriate content
- Nursery devices are used only for legitimate nursery purposes
- Controls, restrictions, and acceptable use of devices are detailed in the Mobile Phone and Digital Devices Policy, Policy 14

5.1 Device Security

The designated GDPR Officer ensures that:

- Safety settings are enabled on all digital devices to block inappropriate material
- Settings are checked and verified each term
- Antivirus and security software is installed and maintained on all nursery systems where applicable
- Device faults or security concerns are reported and addressed promptly

5.2 Staff and Nursery Devices

All staff devices are centrally managed by Peques Head Office. Devices are restricted to approved applications and nursery-related use only. Staff may not install, remove, or modify applications or settings. Personal devices are not permitted in children's areas. Full details are set out in the Mobile Phone and Digital Devices Policy, Policy 14.

6. Children's Access to Digital Devices

Children never have access to staff computers, office-based systems, or staff digital devices at any time.

Children do not independently use or handle digital devices in the nursery. 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. Children do not handle or operate the device independently.

Children do not have access to:

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

All educational content shown to children is carefully vetted and approved by management in advance. No additional software, applications, or content may be installed or accessed without authorisation from Head Office.

7. The Peques Digital Platform and Online Safety

Peques operates the Peques Digital Platform, a centrally governed AI support system for staff. The platform is a controlled internal system, not an open internet tool. The following safeguards are built into its design:

- Teaching and kitchen staff have no internet access through the platform - this is a deliberate safeguarding control

- Management and administration staff have restricted internet access for regulatory research purposes only
- No personal or identifiable data relating to children, families, or staff is entered into any tool
- Children are never involved in or exposed to the platform in any form
- All tools operate under Peques Policies and Procedures as their supreme authority

The Peques Digital Platform is the only AI system approved for use by Peques staff. Use of any external AI tool or internet-based AI service is not permitted. Full details are set out in the Artificial Intelligence (AI) Policy, Policy 7.

8. Staff Responsibilities

All staff are responsible for maintaining vigilance, following this policy, and reporting concerns without delay.

Staff must:

- Use digital devices and online tools only for approved, nursery-related purposes
- Never access personal accounts, social media, or external websites on nursery devices
- Never use personal devices in children's areas during operating hours
- Never photograph or record children using personal devices
- Never share children's images, names, or information through any digital channel outside approved systems
- Supervise children appropriately whenever digital content is used
- Report any online safety concern immediately to the Designated Safeguarding Lead or Manager
- Never ignore, minimise, or delay action where online harm may be present

8.1 Data Protection

Staff must not store children's images or personal data on personal devices, cloud services, or any system not approved by Peques Head Office. All digital records are managed in line with UK GDPR and the Peques Privacy Notice. Children's learning updates and images are shared with parents only through Famly, the approved parent-facing platform.

8.2 Use of AI Tools

Staff may only use the Peques Digital Platform for AI support. The use of any external AI tool, whether on a personal device, personal account, or nursery device, is not permitted. No information about children, families, or colleagues may be entered into any AI system. Full requirements are set out in the Artificial Intelligence (AI) Policy, Policy 7.

9. Children's E-Safety Education

Children's exposure to digital technology is carefully managed and always supervised by staff.

Online safety messages are taught in an age-appropriate and developmentally suitable way through adult modelling, discussion, stories, play-based learning, and everyday interactions.

Children are supported to understand simple stay-safe principles, including:

- Only going online with a trusted grown-up
- Being kind and respectful online
- Keeping personal information private
- Only pressing buttons or links they understand
- Telling a grown-up if something makes them feel unhappy or unsure
- Asking for help and never keeping secrets

These messages are embedded naturally into daily practice rather than delivered as formal instruction.

10. Online Harm, Abuse and Exploitation

Children may be harmed through online content, online contact, online conduct, or online exploitation. Online harm may include exposure to inappropriate or abusive material, grooming, coercion, harassment, sexual exploitation, image-sharing, or other unsafe online experiences.

Online harm may affect children directly or indirectly, including through their home environment, the behaviour of adults, the sharing of content, or wider family and community circumstances.

Staff must remain alert to signs, behaviours, comments, disclosures, or patterns of concern that may indicate a child is being affected by online harm. Any such concern must be treated as a safeguarding matter and escalated immediately in line with the Safeguarding Children Policy and Procedure.

11. Images of Children

The distribution of images of children outside approved Peques systems is strictly prohibited under EYFS regulations. Sharing indecent images of children is a criminal offence.

- Children's photographs and videos are taken only on nursery-owned, centrally managed devices
- Images are shared with parents only through Famly
- Images are never stored on personal devices, personal cloud services, or external platforms
- Editing or altering children's images using AI or digital tools is not permitted
- Parents may photograph their own child at nursery events only in line with the conditions set out at registration and the Social Media & Networking Policy, Policy 15

12. Extremism and Radicalisation

Peques recognises that online environments can be a source of extremist or harmful material. Although children in the early years are unlikely to independently access such content, risks may arise through digital media, family contexts, wider community exposure, or the online behaviour of adults.

Staff are trained to remain vigilant to signs that a child or family may be exposed to extremist, radicalising, hateful, or otherwise harmful online material.

Any concerns relating to extremist material, radicalisation, or online content that may incite hatred or harm must be reported immediately in line with the Safeguarding Children Policy and Procedure and the Prevent Duty.

13. Reporting Concerns

Safeguarding concerns always take priority.

Any staff member, parent, or carer who suspects inappropriate behaviour related to digital safety must act immediately:

- Report to the Designated Safeguarding Lead or Manager on duty without delay
- Follow the Peques Safeguarding Policy and escalation procedure
- Do not investigate independently or attempt to resolve the concern without involving the DSL
- Where a child may be at immediate risk, call 999

Concerns about an adult attempting to make inappropriate online contact with a child must be treated as a safeguarding matter and escalated immediately.

Any concern relating to the creation, possession, viewing, or sharing of indecent images of children must be treated as a serious safeguarding matter.

Where appropriate, concerns may also require reporting to external agencies including the police, the Internet Watch Foundation (IWF), the National Crime Agency's Child Exploitation and Online Protection command (CEOP), children's social care, or Prevent partners.

Concerns relating to staff digital conduct, unauthorised device use, or AI misuse should be reported to the Manager or Head Office. All reports are treated with confidentiality and acted upon promptly.

14. Roles and Responsibilities

Management is responsible for ensuring that:

- Appropriate systems, controls, and oversight are in place across both settings
- Nursery devices are configured and used safely
- Staff receive appropriate induction, training, and updates on digital safety
- Online safety forms part of the nursery's wider safeguarding practice

Head Office holds sole authority over device configuration, platform access, and system monitoring. Managers supervise day-to-day practice but do not hold authority over system configuration or monitoring.

15. Monitoring

Digital device use is monitored at system level by Peques Head Office. The GDPR Officer reviews digital device safety settings each term. Any concerns identified in relation to device safety, online access, system misuse, or inappropriate material must be reported without delay.

16. Breaches of Policy

Breaches of this policy may be treated as misconduct or gross misconduct and may result in disciplinary action, safeguarding investigation, and external referral where required. All breaches are reviewed by Head Office and the Designated Safeguarding Lead.

17. Training and Review

This policy forms part of staff induction and ongoing safeguarding training. It is reviewed annually and additionally following any change in statutory guidance, legislation, Ofsted inspection framework, or digital safety incident.

This policy should be read in conjunction with:

- Safeguarding Children Policy & Procedure
- Confidentiality & Information Sharing Policy
- Mobile Phones & Digital Devices 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