Kenilworth Nursery School
&
Whitnash Nursery School

"Recognising and valuing the uniqueness of every child"

Online, Mobile Phone, Camera and Smart Device Policy

Maintained nursery school federation | 2026–2027

Status	**Approved December 2026**
Policy owner	Headteacher: Rachel Barber
Approved by / date	Alison Paveley November 2026
Effective from	Following governing body approval
Review date	November 2027, or sooner following an incident or significant change
Version	1.1 | Revised 2 November 2026

Statement of intent and scope

Kenilworth Nursery School and Whitnash Nursery School will use technology safely, securely and sparingly to support children's learning, communication and welfare. Responsive relationships, play, movement, outdoor experiences and first-hand exploration remain central to our provision for children aged 12 months to 4 years.

This policy applies across both schools and on visits to employees, governors, students, volunteers, supply staff, contractors, parents, carers and visitors. It covers mobile phones, cameras, tablets, laptops, interactive displays, smart watches, wearable devices and connected toys, including devices capable of recording, imaging or sharing information.

Read this policy alongside our Child Protection and Safeguarding Policy, Cyber Security Policy, Data Protection and GDPR policies, Privacy Notice, Staff Code of Conduct and SEND arrangements. Safeguarding concerns follow the safeguarding policy; technical incidents follow the cyber response procedure; personal data breaches also follow the data protection procedure. One incident may require all three responses.

EYFS 2026 requirements and local procedures

The EYFS statutory framework for group and school-based providers effective from 1 September 2026 applies to our provision. Paragraph 3.94 introduces the requirement to have regard to DfE guidance on children's screen use. Section 8 below explains how we implement that duty. The guidance informs our decisions; its age-related advice is not a separate statutory daily screen-time allowance.

The framework also requires safeguarding procedures consistent with local safeguarding partners' guidance (paragraph 3.5), rules for devices with imaging and sharing functions (3.6), safeguarding leadership and reporting (3.4 and 3.9), and secure, confidential records (3.95–3.98). These continuing requirements underpin this policy; they are not all new in 2026.

We will use Warwickshire County Council's Early Years Online Safety Audit and associated resources to review practice at both schools and Warwickshire Safeguarding Partnership procedures for child protection, allegations and escalation. We follow applicable Warwickshire information security requirements, ICT guidance and county breach procedures, including requirements in purchased services; where these impose a higher standard, that standard applies.

Responsibilities

- The governing body approves this policy, oversees safeguarding and digital risks, and checks that leaders have sufficient support and resources.
- The Headteacher ensures consistent practice across both sites, authorises devices and systems, and coordinates significant incident responses. Any delegated online safety role is recorded, with cover arrangements.
- Rachel Barber, Headteacher and lead DSL for both schools, is the Online Safety / Filtering and Monitoring Lead, supported onsite by the DDSLs. The DSL leads online safeguarding, assesses risks to children, oversees safeguarding responses to monitoring alerts and liaises with statutory services. Delegating administration or technical work does not transfer this responsibility.

- WES, the contracted IT provider, implements agreed technical protection, investigates faults and cyber incidents, and provides evidence of filtering and monitoring effectiveness. The Warwickshire DPO advises on lawful processing, privacy, suppliers and breach notifications.
- All staff follow this policy, actively supervise children, protect information and report concerns immediately. The SENCO supports individual communication and access arrangements.

Photography video and digital learning records

Only authorised staff may record children using approved school-owned devices and school accounts. Personal phones, cameras, wearables and personal cloud storage must never be used to record or store children's images, audio or records. We take only what is necessary for an identified educational purpose; photographs are not required for every observation or milestone.

Before recording or sharing, staff check the purpose, audience, current permissions and any safeguarding restrictions. Routine learning records and optional publicity have distinct purposes and lawful bases under our Privacy Notice. Separate, informed consent is required for optional publicity; refusal must not affect provision. Staff respect a child's distress or objection and do not photograph intimate care, undress or situations compromising dignity.

Images and observations may support reflection, assessment, moderation, transition and communication with families through the approved learning journal. Staff must check who appears in each image, prevent disclosure of another child's confidential information and verify recipient access, including relevant court orders or safeguarding restrictions. Images must not be accompanied by unnecessary identifying or location information.

We use UK GDPR and the Data Protection Act 2018 when collecting, sharing and retaining records. Necessary safeguarding sharing must not be delayed solely to obtain consent. Refer rights requests and disputed access or consent decisions to the Headteacher and DPO.

Learning journals device storage and cyber security

- Use only the approved learning journal and school communication systems, with individual accounts and role-based access. Personal devices must not access children's learning journals or records under this policy; use a managed school device for authorised remote work. This restriction applies to children's images and records even where the Cyber Security Policy permits an approved personal device for other work.
- Use strong unique passwords and multi-factor authentication where available, in line with the Cyber Security Policy. Never share credentials. Lock screens when unattended and keep devices securely stored.
- School iPads must have at least a six-digit passcode, automatic locking and managed security settings agreed with IT support.
- Prevent automatic syncing to personal accounts or camera rolls.
- School devices remain on site unless the Headteacher authorises a visit or another school purpose. Record who holds an off-site device and apply the cyber policy's secure transport and remote working arrangements.

- Do not install unapproved apps, use personal email or messaging for children's records, transfer images outside approved systems or disable security controls. Staff must check recipients, attachments and sharing permissions before sending.
- IT support will manage supported software, updates, restricted child access, backup and recovery, and secure disposal under the Cyber Security Policy. Remove temporary device copies after secure upload in accordance with the approved retention procedure, unless preservation is required.
- Before introducing a platform, app, connected toy or recording service, obtain Headteacher approval and IT/DPO review of security, data use, processor terms, access, transfers and retention. Complete a data protection impact assessment where required. Do not enter identifiable school information into public AI tools, unless using the closed system Co-Pilot through your welearn365 account.

6 Personal phones smart watches and wearables

Staff store personal phones in the designated staff area and use them only during breaks away from children. An exceptional emergency use requires senior leader authorisation and safe cover for supervision. It never permits recording children or accessing their records. Emergency contact arrangements must be explained at induction and before visits.

A smart watch may be worn only with calls, messaging, notifications, imaging, recording and sharing functions disabled during work with children. A device that cannot meet these controls must be removed and securely stored. Agree any disability or medical adjustment with the Headteacher through a recorded risk assessment that protects children and privacy.

Students, volunteers, contractors and visiting professionals receive the same device restrictions. Authorised work by an external professional using their own organisation's equipment requires prior senior leader agreement, a clear purpose, appropriate permissions and secure handling; it is not permission to use a personal phone.

Educational use of technology

Technology may support a specific learning experience, such as exploring an image together, making a short recording of a child's creation or supporting communication. Staff first consider whether a real object, book, conversation, outdoor investigation or other practical experience would meet the aim better. There is no expectation that children complete digital tasks to demonstrate EYFS progress.

Children use only approved school equipment with restricted access that cannot expose staff records. An adult stays with them, talks with them and controls access. Assessment relies on professional observation and judgement, without screen-based tests for nursery children. Staff recording or uploading observations must remain brief and must never interrupt safe supervision or sustained interaction.

Screen time and screen use

We have regard to DfE's Help for early years providers screen-use guidance. For under-twos we avoid screen time. For ages two to four, the advice is no more than one hour across the whole day, preferably less, including home use. This is not a nursery allocation or target. Assistive technology for SEND is excluded from those time limits.

Screen experiences are brief, planned around a clear learning aim and shared with an engaged adult. Content is checked in advance, age-appropriate, calm and advert-free, with autoplay and scrolling disabled. Children do not use screens unsupervised. We avoid children's use of AI, including AI toys.

Screen use must not displace physical play, outdoor time, stories, sleep or relationships. Adult device use and assessment recording must be proportionate and keep attention on children. We discuss family screen habits sensitively and share practical advice. These arrangements implement the guidance through the following federation controls.

- Before any planned screen activity, the practitioner identifies its purpose, intended duration, adult support and suitable non-screen alternative. Use the shortest period needed; stop when children disengage or become unsettled.
- Screens are not used as background television, routine entertainment, a reward, a behaviour management tool or a replacement for staff interaction at meals, settling or transitions.
- Do not conduct live unrestricted web or image searches in front of children. Prepare approved material in advance, using secure offline resources where appropriate. Children must not access open video feeds, chat, advertising or purchase functions.
- The SENCO agrees individual use of communication aids and other access technology with families and relevant professionals. Record the purpose and support in the child's plan and review its benefit; do not withdraw essential communication access to meet a general screen limit.
- Key people review screen use through planning and routine observation, including total use during a nursery day, educational value and impact on engagement. The Headteacher reviews exceptions and patterns termly without creating unnecessary individual tracking.

Online safety filtering and monitoring

Safeguarding and prevention

Online safety is part of our safeguarding practice, including risks encountered at home. Staff remain alert to harmful content, unwanted contact, unsafe sharing, exploitation, scams and commercial pressure. Children's age, development, communication needs and vulnerability inform our response; technical controls do not replace adult supervision.

Through ordinary play and conversation, adults model asking permission before taking a photograph, keeping personal information private, stopping when something unexpected appears and asking a trusted adult for help. Use simple words and visual support for children with SEND or emerging language. Children are not responsible for managing online risks themselves.

Filtering and monitoring arrangements

The Headteacher, DSL and WES will document which devices, networks and services are covered, who receives alerts, who checks them and how urgent concerns are escalated, including absence cover. Filtering and monitoring must be appropriate for nursery users and reviewed at least annually and

following significant changes or incidents. The governing body receives assurance on effectiveness and unresolved risks.

Staff must not bypass protection, use personal hotspots or connect unapproved equipment. Guest and personal connections must not give children an unfiltered route or access to confidential systems. Report blocked educational resources through the approved review process; never disable a control. Monitoring is proportionate, access restricted and its purposes explained through acceptable use information and privacy notices.

We will use Warwickshire's Early Years Online Safety Audit to review supervision, device controls, staff awareness and work with families. Record actions, owners and completion dates across both sites. Staff receive induction and at least annual online safety updates, alongside safeguarding and cyber training, and know how to report concerns or unsafe adult practice.

Promoting Online Safety at Home

We work in partnership with parents and carers to promote safe, balanced use of technology at home. Through newsletters, our websites, conversations and parent sessions, we share practical guidance on choosing age-appropriate content, setting parental controls, protecting children's photographs and personal information, and enjoying digital activities together. We encourage families to keep screen use limited and purposeful, prioritising conversation, play, outdoor experiences and sleep. We signpost parents to Warwickshire County Council's online safety resources and offer sensitive, non-judgemental support. Parents are encouraged to speak to their child's key person or the Designated Safeguarding Lead if they have concerns about online content, contact or their child's use of technology.

Responding to online safeguarding concerns

If inappropriate content appears, stop children viewing it, reassure and supervise them, and report immediately to a DSL. Report urgent concerns verbally to the DSL/DDSL without delay, then record factual details, time and actions in CPOMS. An electronic entry does not replace direct communication or checking that an urgent report has been received. If CPOMS is unavailable, use the approved green paper concern form and arrange secure transfer into CPOMS when restored, retaining the original under the retention procedure. Staff must not investigate suspected abuse, repeatedly view material, or copy, screenshot or forward suspected child sexual abuse imagery. Preserve the device securely and follow DSL, police and IT advice.

The DSL assesses the child's safety and follows the Child Protection and Safeguarding Policy and Warwickshire referral procedures. Do not wait for a technical investigation before safeguarding action. If the DSL is unavailable, follow the safeguarding escalation route; any member of staff can make a referral. Concerns about staff go to the Headteacher, or to the Chair of Governors where the concern is about the Headteacher. Follow low-level concern, allegation, LADO and whistleblowing procedures as applicable.

For a child protection concern, Warwickshire Family Connect can be contacted on 01926 414144; for an out-of-hours emergency use 01926 886922. Call 999 for immediate danger. Use the current Warwickshire referral and threshold procedures linked in section 12; contact details must be checked at each review.

Cyber incidents and personal data breaches

Immediately report a lost device, compromised account, suspicious message, unauthorised image sharing, incorrect disclosure or filtering failure to the Headteacher and Warwickshire DPO, in line with section 12 of the Cyber Security Policy and involve WES promptly for technical support. Involve the DSL wherever children may be at risk. Use a trusted telephone route if school email is compromised; do not rely on leaving an unchecked message.

Stop using the affected equipment. For suspected malware, disconnect from the network if safe and follow the Cyber Security Policy and IT instructions. Do not reset, wipe, delete evidence or attempt repairs. Record discovery time, what happened and actions taken. Secure evidence with restricted access without circulating harmful or confidential material.

The Headteacher coordinates containment, continuity and external reporting. The controller, advised by the DPO, records and assesses every personal data breach and notifies the ICO without undue delay and, where feasible, within 72 hours of awareness unless it is unlikely to risk individuals' rights and freedoms. High-risk breaches also require notification to affected people without undue delay, subject to lawful exceptions. Safeguarding, contractual and Council reporting duties are considered in parallel.

Families and visitors

Parents, carers and visitors are asked to put phones away in areas used by children and seek staff guidance if a call is necessary. No photography or recording is permitted without school agreement. At authorised events, families follow the school's arrangements, avoid recording other children and must not publish identifiable images of other children online. Staff may stop recording where privacy or safeguarding is at risk. No recording is permitted in toilets or changing areas.

Children should not bring personal connected devices or camera watches into nursery. Agree any essential medical or communication equipment with the Headteacher and SENCO individually, retaining safe access to necessary support. This policy will be shared with families through admissions documents and is available to view on our websites.

The Headteacher and DSL monitor implementation at both schools. Termly review considers incidents, staff training, screen-use practice, access and permission checks, audit actions and IT assurance. Significant issues go to governors. We will review this policy annually or sooner after an incident or changes to EYFS, safeguarding, data protection or Warwickshire procedures.

References and linked procedures

DfE EYFS statutory framework for group and school-based providers from September 2026, particularly paragraphs 3.4–3.6, 3.9, 3.94 and 3.95–3.98

https://www.gov.uk/government/publications/early-years-foundation-stage-framework--2

DfE Help for early years providers Screen use, updated 7 September 2026

https://help-for-early-years-providers.education.gov.uk/health-and-wellbeing/screen-use

DfE Help for early years providers Internet safety

https://help-for-early-years-providers.education.gov.uk/health-and-wellbeing/internet-safety

DfE Keeping children safe in education current statutory guidance

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Warwickshire County Council Early Years Online Safety resources including audit and parent guide

https://schools.warwickshire.gov.uk/safeguarding-early-help/safeguarding-welfare-1/12

Warwickshire Safeguarding Partnership school policy guidance and image consent resources

https://www.safeguardingwarwickshire.co.uk/safeguarding-children/policies-and-procedures-for-schools/

Warwickshire County Council report child abuse concerns

https://www.warwickshire.gov.uk/childprotection

Warwickshire County Council concerns about a person in a position of trust and LADO procedures

https://www.warwickshire.gov.uk/childrens-social-care/child-safeguarding-procedures-professionals/4