

63. Online Safety and Screen Use Policy

Policy Statement:

St Vincent's Nursery is aware of the growth of internet and technology and the advantages this can bring to everyday life. While it offers valuable educational opportunities, we are committed to protecting children, staff and families from online risks and ensuring the responsible, safe and positive use of digital technology.

This policy forms part of our wider safeguarding approach and should be read alongside our Safeguarding Children Policy, Acceptable Use Policy and Data Protection Policy.

We refer to '[*Safeguarding children and protecting professionals in early years settings: online safety considerations*](#)' to support this policy.

From 1st September 2026, the Early Years Foundation Stage (EYFS) requires providers to have regard to the Department for Education's *Screen use guidance for early years settings*. St Vincent's Nursery adopts a precautionary approach to screen use and ensures that any use of screens with children is limited, purposeful, developmentally appropriate and clearly linked to children's learning and development.

This policy applies to all staff, students, volunteers, visitors and parents using digital technologies in relation to St Vincent's Nursery. It covers all nursery-owned devices, systems and online platforms, as well as personal devices used on nursery premises.

Aims and Objectives:

Our aims are to:

- Safeguard children from potential harm arising from online activity or exposure to inappropriate content.
- Support staff to use digital technology safely, responsibly and professionally.
- Promote children's early understanding of safe technology use.
- Work in partnership with parents and carers to reinforce online safety messages.

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Ivana Butterworth**.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation with technology often providing the platform that facilitates harm.

The breadth of issues included within online safety is considerable, but can be categorized into four areas of risk:

- ✓ **Content:** being exposed to illegal, inappropriate or harmful material; such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- ✓ **Contact:** being subjected to harmful online interaction with other users; such as child-to-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- ✓ **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- ✓ **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams

How We Keep Children Safe:

Children are introduced to basic online safety concepts through play, stories and discussions appropriate to their age and understanding (e.g., asking for help, keeping information private). Within the nursery we aim to keep children, staff and parents safe online. Our safety measures include:

- Ensuring we have appropriate antivirus and anti-spyware software on all devices and update them regularly
- Ensuring content blockers and filters are on all our devices, e.g. computers, laptops, tablets and any mobile devices
- Ensuring all devices are password protected and have screen locks. Practitioners are reminded to use strong, unique passwords / passphrases and MFA where available, with passwords changed where compromise is suspected
- Monitoring all internet usage across the setting
- Providing secure storage of all nursery devices at the end of each day
- Ensuring no social media or messaging apps are installed on nursery devices
- Reviewing all apps or games downloaded onto devices ensuring they are age and content appropriate
- Using only nursery devices to record / photograph children in the setting; photographs and videos will be kept to the minimum necessary for legitimate educational, assessment or communication purposes and will only be shared with parents through approved, technically secure nursery systems
- Only transmitting personal, confidential or financial information using approved secure systems and in accordance with the nursery's Data Protection Policy
- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Teaching children how to stay safe online and report any concerns they have
- Ensuring children are supervised when using internet connected devices
- Using tracking software to monitor suitability of internet usage (for older children)
- Only permitting staff or visitors to access to the nursery Guest Wi-Fi
- Talking to children about 'Clever Never Goes' and deciding who is safe and who is not; comparing people in real life situations to online 'friends'

- When using online video calls or video-conferencing platforms (where applicable) discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff, at least annually, in online safety and understanding how to keep children safe online
- Staff modelling safe practice when using technology with children and ensuring they abide by an Acceptable Use Policy, such as instructing staff to use the nursery IT equipment for matters relating to the children and their education and care only
- Making sure the physical safety of users is considered including the posture of staff and children when using devices
- Being aware of the need to manage our digital reputation, including the appropriateness of information and content that we post online, both professionally and personally. This is continually monitored by the setting's management
- Ensuring that staff do not friend or communicate with parents on personal devices or social media accounts
- Ensuring all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses and telephone numbers. This is to protect staff, children and parents
- Signposting parents to appropriate sources of support regarding online safety at home

Screen Use in the Nursery:

St Vincent's Nursery recognises that children's development is best supported through real-world experiences, active play, exploration, communication and responsive interactions with adults and other children. Screens will therefore be used sparingly and will not replace high-quality interactions and first-hand learning experiences.

In accordance with the EYFS and Department for Education *Screen use guidance for early years settings*, we adopt a precautionary approach to children's screen use.

Children under two years of age will not routinely use or view screens. Screen use will only take place in exceptional circumstances where there is a clear benefit to the child, for example a video call with a parent or carer.

For children aged two to five, screen use within the nursery will be limited and kept as short as possible. Any screen-based activity must have a clear learning or developmental purpose and will form only a small part of the child's overall day. Practitioners will be mindful that children may also use screens at home and that the DfE recommends no more than one hour of screen time per day for children aged two to five, with less being preferable.

Where screens are used, practitioners will actively engage with children by talking, questioning, commenting and encouraging children to think and respond. Passive viewing will not form part of our routine provision.



Screen use will not replace physical activity, outdoor play, sleep, stories, creative experiences, social interaction or responsive adult-child engagement.

Before using any screen-based content with children, practitioners will consider its purpose, quality, pace, age appropriateness and potential developmental benefit. Content described or marketed as 'educational' will not automatically be assumed to be suitable.

Screens will not routinely be used:

- during mealtimes
- within one hour of a child's sleep period
- as background entertainment
- to occupy children during transitions or waiting periods
- to calm children or manage behaviour
- as a substitute for interaction with a practitioner
- where an equivalent high-quality, screen-free experience can reasonably be provided

Children with SEND:

Screen-based assistive technology may be used where it supports a child's communication, accessibility, independence, well-being or individual needs. The general screen-time recommendations within this policy do not apply to assistive technologies used by children with SEND. Their use will be considered according to the individual child's needs and, where appropriate, their support plan.

Children's Personal Devices:

Children will not normally bring or use personal internet-connected or screen-based devices at nursery. Where an individual need requires a child to use a personal device or assistive technology, this will be agreed with parents and managed through an individual risk assessment where appropriate.

Responsibilities of All Staff:

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the nursery's ICT systems and the internet
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures by logging it if they need to bypass the filtering and monitoring systems for educational purposes



- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the nursery's Staff Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Practitioners will keep their own use of nursery digital devices in children's presence to the minimum necessary. Recording observations, assessments and communications will be completed proportionately and in short periods so that use of devices does not detract from supervision, interaction or engagement with children.

Acceptable Use of the Internet:

All staff and volunteers are expected to sign an agreement regarding the acceptable use of the nursery's ICT systems and the internet. Visitors will be expected to read and agree to the nursery's terms on acceptable use if relevant.

Use of the nursery's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by staff, volunteers and visitors (where possible) to ensure they comply with the above and restrict access through filtering systems where possible and appropriate.

Artificial Intelligence (AI):

Children will not directly use generative AI tools, AI chatbots or toys with built-in AI features as part of the nursery's early years provision. In accordance with current DfE guidance, we will avoid children's direct use of AI until there is stronger evidence regarding its impact on young children's development.

Responding to Concerns:

If any concerns arise relating to online safety, then we will follow our safeguarding policy and report all online safety concerns to the Designated Safeguarding Lead.

The DSL will make sure that:

- All staff know how to report a problem and when to escalate a concern, including the process for external referral
- All concerns are logged, assessed and actioned in accordance with the nursery's safeguarding procedures



- Parents are supported to develop their knowledge of online safety issues concerning their children
- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern.
- Staff have access to information and guidance for supporting online safety, both personally and professionally
- Under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material.
- The DSL will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Cyber Security:

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the [Data Protection Act](#). We are aware that Cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity e.g. scam emails. All staff are reminded to follow all the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

We will:

- Use strong passwords, updated regularly, for all digital systems.
- Restrict access to data and systems on a "need to know" basis.
- Ensure antivirus, firewall and software updates are maintained on all devices.
- Store backups securely and test them regularly.
- Protect all online accounts with multi-factor authentication where possible.
- Use secure, encrypted connections for data transfers and communications.
- Report suspected data breaches immediately to the Nursery Manager and DSL, who will follow the data breach procedure.
- Provide regular cyber security awareness training to staff, including recognising phishing emails, managing passwords and avoiding malicious links.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with, we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the Nursery Manager as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious Email Reporting Service at report@phishing.gov.uk



St Vincent's Nursery, Orchard Road, Altrincham, Cheshire, WA15 8EY

Policy reviewed:

1st September 2026

Reviewed by:

Ivana Butterworth