Online Safety in Early Years 2026-2027

Reviewed: 22nd October 2026

Introduction

This Online Safety Policy has been developed to safeguard children and staff within our setting. Online safety is highlighted within the Early Years Foundation Stage (EYFS) and Early Years Inspection Handbook and is especially important in early years, as our youngest children won't ever know a world without technology, so good strategies must be embedded from a young age. Good habits and knowing how to keep safe are fundamental from the start of a child's journey.

Keeping Children Safe in Education states:

"The breadth of issues classified within online safety is considerable but can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material.
- **Contact:** being subjected to harmful online interaction with other users; and
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm."
- **Commerce:** the risk from online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly.

***Safeguarding children and protecting professionals in early years settings: online safety guidance for practitioners'* states:**

'You play an essential role in helping young children learn the foundations of safe online behaviour. Even if children don't have access to technology within your setting, they will/ may be using it at home, with their friends or in other public spaces. Children are naturally curious in understanding the world we live in; it is our responsibility to enable them to do so, including helping them to recognise the value of technology and use it safely. Role modelling safe use of the internet should become part of our everyday practice'.

Aims

The aims of this policy are:

• Ensure the safety and wellbeing of children is paramount when adults or children are using the internet, social media or mobile devices.

• Provide staff, students and volunteers with the overarching principles that guide our approach to online safety.

• Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. The policy statement applies to all staff, volunteers, children, and anyone involved in Sir James Knott Nursery School and Nest activities.

Principles

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

The key principles below around digital media use and online safeguarding highlight how we aim to keep our young children safe online:

- In our setting, digital media will be used when there is a clear link to supporting child development. Any other use of digital media will be avoided. Staff will be supported to understand about developmental digital media use
- Technology use does not replace or interfere with adult or child interactions
- Staff will always support children when using digital media, to promote and scaffold learning
- Our setting has appropriate technical systems in place to keep children safe online, including broadband and device safety controls to limit access to unsuitable content
- Our setting has a robust online safeguarding policy which is reviewed annually to include local and national trends, and which highlights the setting's principles and approach to keeping children safe online
- Our setting has an explicit approach to limit children's passive consumption of online content
- All staff in our setting access regular safeguarding training, which includes online safeguarding - learning about the risks of using devices and staff's responsibilities in keep children safe online
- Staff in our setting role model positive and balanced use of technology and there are behaviour policies in place to create clear boundaries for staff's use of technology
- Our setting has a proactive approach to supporting parents and carers with keeping children safe online when at home

The Designated Safeguarding Lead is the John Croft- Headteacher supported by Nicki Battensby- School Business Manager. They are ultimately responsible for online safety concerns. All concerns must be raised to the Headteacher/School Business Manager as soon as possible.

The Designated Safeguarding Leader (DSL) will be accountable for:

- Ensuring online and offline safeguarding concerns are addressed - helping young children explore safely with adult guidance, to ensure positive digital experiences
- Determining appropriate responses to concerns - assessing safeguarding issues in consultation with the Deputy Designated Safeguarding Lead for Online Safety and determining whether concerns involve online risks
- Referring cases to authorities - reporting suspected abuse or safeguarding breaches, including cases involving online exploitation or cyber-related offences, to social care services or the police
- Monitoring secure and accurate records - documenting referrals and safeguarding concerns, ensuring records of online safety issues are securely stored and shared appropriately
- Providing advice and guidance on safeguarding - educating staff and volunteers about online safety risks and digital safeguarding measures, including preventing exposure to harmful content and securing personal data
- Keeping up-to-date with safeguarding legislation - staying informed about changes in safeguarding regulations, particularly laws relating to online safety, digital data protection and child online protection policies

The Deputy Designated Safeguarding Lead (DDSL) for Online Safety will be accountable for:

- Supporting the DSL and other deputies in safeguarding children - assisting in ensuring the safety and welfare of individuals within the organisation, including protection from online risks and harmful online content
- Implementing safeguarding policies in partnership with the DSL, including online safety - helping integrate online safety measures and promoting responsible use of technology and social media within the organisation
- Providing advice on online and offline safeguarding matters - guiding staff on identifying and addressing online safeguarding concerns
- Maintaining accurate records of safeguarding concerns - documenting online safety incidents, alongside other safeguarding records
- Assisting the DSL with referrals for online and offline abuse cases - supporting the referral of safeguarding concerns
- Ensuring continuity in safeguarding responsibilities - stepping in for the DSL when necessary, overseeing both offline and online safeguarding efforts to ensure consistent protection for all individuals

Our safety measures include:

Ensuring we have appropriate antivirus and anti-spyware software on our network computers connected to the network, updated and monitored by the IT team.

• Keeping passwords safe and secure. IT team will prompt staff to change their passwords on regular basis

• Locking away all Nursery devices at the end of the day

• Using approved devices to record/photograph in the setting as selected by the IT team

• Reporting emails with inappropriate content to the IT team

• Ensuring children are supervised when using internet devices

• Restricting access to the Wi-Fi to approved staff and visitors

• Talking to children about 'stranger danger' (age-appropriate) and deciding who is a stranger and who is not, comparing people in real life situations to online 'friends'

• Staff are requested to complete online safety regularly, prompted by the IT department, supporting understanding how to keep children and staff safe online

• We abide by an Acceptable Use policy; ensuring staff only use the work IT equipment for matters relating to the children and their education and care and not personal use

• Children's screen time is monitored to ensure they remain safe online and have access to material that promotes their development. We will ensure that their screen time is within an acceptable level and is integrated within their programme of learning

• All staff know how to report a problem and when to escalate a concern

• All concerns are logged, assessed and actioned upon using the Safeguarding procedure

• Staff can signpost parents to appropriate sources of support regarding online safety at home and help them to understand how to report an online safety concern

Cyber Security for Safeguarding in Early Years

Cyber security is essential to safeguard all the devices we use and to protect our information, most of which is sensitive concerning our children, their families and staff. In line with legislation, only people with a professional need and who are authorised should access these records. They must remain confidential and protected.

- All information must be backed up, either on the cloud, with password or other ID protection
- Strong passwords will be used to control access to relevant documents and information on all devices, including folders on computers. Only authorised people will be able to access information, and when sending information to parents or professionals, a password system will be created so only they can open it
- All devices have protective software from viruses and malware which are regularly kept up to date
- Staff will be trained on how to recognise and deal with suspicious messages or contact

- Staff will be knowledgeable about legislation and requirements and know where to go for advice and how to deal with breaches

Online guidance and resources for parents and practitioners

- https://safeguarding.network/content/online-safety-advice-for-early-years-settings
- Safeguarding children and protecting professionals in early years settings: online safety
- guidance for practitioners - GOV.UK
- Pre-school (0-5) online safety tips and advice | Internet Matters

We encourage staff and families to utilise the following online teaching tools to support children with online safety:

- https://www.childnet.com/resources/smartie-the-penguin/

- https://www.childnet.com/resources/digiduck-stories/

Relevant Policies

This policy will be read in conjunction with the following policies:

- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Staff handbook
- Code of conduct

Nursery/School name: Sir James Knott Nursery School and Nest

Date of policy review: 22.10.26

Date of next review: October 2027

The named persons for drawing up and leading the review of this policy are: John Croft