

# Online Safety Policy



|                     |                               |
|---------------------|-------------------------------|
| Implementation Date | September 2026                |
| Review Date         | September 2027                |
| Reviewer            | Liam Donovan/Alison Lapihuska |

We are aware of the growth of the internet and the advantages this can bring. However, it is also aware of the dangers it can pose, and we strive to support children, staff and families to use the internet safely.

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

The Designated Safeguarding Lead (DSL) has overall responsibility for online safety within the school/nursery and any online safety concerns must be reported to them as soon as possible.

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 categorised into three areas of risk:

**Content:** *being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views*

1. **Contact:** *being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults, and*
2. **Conduct:** *personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.*

## Artificial Intelligence and Emerging Technology

The school/nursery recognises that advances in technology may create new safeguarding risks. These include artificial intelligence (AI), AI-generated imagery, deepfakes, image-based abuse, online manipulation, technology-facilitated coercion, and other emerging digital risks.

Staff will receive safeguarding updates and training to help identify, assess, and respond appropriately to these emerging risks. The nursery will regularly review its online safety procedures to ensure they remain effective in response to technological developments.

# Online Safety Policy



Within the school/nursery we aim to keep children, staff and parents safe online. Our safety measures include:

- All staff are responsible for maintaining professional boundaries online, reporting online safety concerns promptly, and ensuring that technology is used safely, securely, and appropriately at all times.
- Staff must be mindful of their online presence and understand that content shared online, whether professionally or personally, may impact their professional reputation, suitability to work with children, and the reputation of the school/nursery.
- 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 complex strong passwords, keep them safe and secure, change them regularly and not to write them down
- The school/nursery uses appropriate filtering and monitoring systems to help safeguard children and staff when accessing online content. These systems are reviewed regularly to ensure they remain effective, proportionate, and appropriate for the needs of the setting.
- Providing secure storage of all nursery devices at the end of each day
- Using only school/nursery devices to record and /or photograph children in the setting
- Ensuring that staff do not use personal electronic devices with imaging and sharing capabilities, including mobile phones, smart watches and cameras during working hours
- Staff must never access online learning platforms and the settings systems (such as FAMLY) outside of working hours, and should never access such systems whilst using personal details at home.
- Never emailing personal or financial information
- Reporting emails with inappropriate content to the internet watch foundation (IWF [www.iwf.org.uk](http://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
- Not permitting staff or visitors private access to the nursery Wi-Fi
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not; comparing people in real life situations to online 'friends'
- When using online video chat, such as Zoom, Teams, Skype, FaceTime etc. (where applicable) ensuring no sensitive information or images are seen
- Discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff in online safety and understanding how to keep children safe online.
- Staff modelling safe practice when using technology with children and ensuring all staff abide by an acceptable use policy such as instructing staff to use the school/nursery IT equipment for matters relating to the children and their education and care only. No personal use will be tolerated (see Acceptable internet use policy)

# Online Safety Policy



- Monitoring children's screen time to ensure they remain safe online and have access to material that promotes their development. We ensure that their screen time is within an acceptable level and is integrated within their programme of learning
  - The school/nursery has regard to the Department for Education guidance 'Help for Early Years Providers: Screen Use' and reviews the use of technology regularly to ensure it remains developmentally appropriate, balanced, and beneficial to children's learning, wellbeing, and development.
  - Making sure the physical safety of users is considered, including the posture of staff and children when using devices
  - Staff must be mindful of their online presence and understand that content shared online, whether professionally or personally, may impact their professional reputation, suitability to work with children, and the reputation of the school/nursery.
- 
- Staff must 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, Family, and telephone numbers. This is to protect staff, children and parents
  - Signposting parents to appropriate sources of support regarding online safety at home

If any concerns arise relating to online safety, then we will follow our Safeguarding children and child protection policy and report all online safety concerns to the DSL.

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
- The DSL will ensure that online safety information, guidance, training materials, and relevant national safeguarding updates are shared regularly with staff and, where appropriate, with parents and carers.
- All concerns are logged, assessed and actioned in accordance with the school/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.

## Cyber Security

# Online Safety Policy



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.

All devices used within the nursery must receive regular software and security updates. Staff must report any suspected cyber security incidents, unauthorised access, data breaches, malware infections, phishing attempts, or loss of devices immediately to management.

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 manager as soon as possible and these will be reported through the NCSC Suspicious email reporting service at [report@phishing.gov.uk](mailto:report@phishing.gov.uk).

## Further Guidance

Early Years Foundation Stage (EYFS) Statutory Framework for Group and School-Based Providers (effective from 1 September 2026)

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

Working Together to Safeguard Children (2026)

<https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Keeping Children Safe in Education (KCSIE) 2026 (although directed at schools, it provides important safeguarding and online safety guidance that early years providers may find useful)

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

Prevent Duty Guidance for England and Wales

<https://www.gov.uk/government/publications/prevent-duty-guidance>

Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations

<https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations-for-managers>

Help for Early Years Providers: Screen Use

<https://help-for-early-years-providers.education.gov.uk/safeguarding-and-welfare/screen-use>

Data Protection Act 2018 <https://www.legislation.gov.uk/ukpga/2018/12/contents>

UK General Data Protection Regulation (UK GDPR) <https://www.gov.uk/data-protection>

## Linked Policies

Safeguarding & Child Protection Policy

Mobile Phones and Electronic Devices Policy

Acceptable IT Use Policy

# Online Safety Policy



Whistleblowing Policy  
Safeguarding Code of Conduct