East Prescot Road Nursery School Online Safety Policy

Designated Safeguarding Lead: Craig Bolton
Designated member of staff for online safety: Craig Bolton
Designated governor for online safety: Julie Nadim

Rationale:

Online safety is especially important in early years as our children will never 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.

Children play online games, use apps, have household items with voice control, and have access to watches and phones, all with online access. Technology is everywhere, and this policy seeks to establish safe practices that, along with parents, ensure that our children stay safe online.

Our children could be at risk of…

- **Content (what they may see):**

Inappropriate images and videos can be stumbled upon by accident by search function or voice control. This can be intimidating, frightening, and harmful. Without proper security and privacy settings, personal information could be revealed as well as accidental spending on games or other purchases.

- **Contact (who might communicate with them):**

Children can be coerced and abused online by strangers as well as people they know, especially in games or chat apps, including video contact. This can range from bullying, unkind words and behaviour, exposure to inappropriate content, control and manipulation, through to the worst forms of abuse.

- **Conduct (how they might behave):**

Early years children, in particular, are vulnerable due to a natural curiosity around their own and others' body parts and are the easiest to manipulate and coerce as they do not have the developed boundaries of older children. They may exhibit unhealthy attachments to screens, use inappropriate language and terminology and form inappropriate friendships with people online who they truly believe are friends. If privacy settings are not at the highest level possible, they can inadvertently share personal information, images taken of themselves or held on the device, and/or financial information and purchases.

- **Strategies we use in school:**

Staff in our school will always:

- supervise children when they are using technology and accessing the internet.
- use devices that belong to the school and never use personal devices.
- check websites, apps and search results, and understand age ratings.
- ensure safety and privacy settings are set at the highest level.
- set age-appropriate time limits.

- model safe internet use and language
- talk to children about keeping safe online and what to do if they are worried.
- If using IT equipment with children and going online, understand and show how it supports children's learning and development and be able to explain this to children, parents and other professionals.
- conduct regular checks of all equipment to ensure appropriate access and use.
- communicate with parents and share information about online safety with them.
- consider what online risks children may be exposed to at home, e.g., vulnerability to radicalisation or other safeguarding risks
- know how to ask for advice when needed and where to find advice online.
- keep up to date through training and research and be aware of the benefits and risks to children.

Use of social media

Using social media can be great but it can carry extra risks for early years practitioners. The boundaries between offline and online can become blurred and this can have serious consequences for professionals.

Staff should be aware of their online conduct and report any issues, including online bullying towards them. They should be aware that their personal digital profile can impact the school. Staff should also discuss with the DSL if they have any pre-existing online friendships or relationships with any family members of the children in their care. This can be managed with appropriate online behaviour guidance on boundaries.

Supporting parents to keep their children safe online

Some parents may not be aware of the risks associated with internet use for pre-school children. Adults often underestimate the knowledge and understanding of younger children and therefore can unwittingly expose them to age-inappropriate material. Some children may be neglected due to parents' excessive use of the internet via phones, games or other preoccupations. Parents can also fail to protect children online if they don't have the appropriate settings and privacy.

Some young children know more than adults and they can be much more proficient at finding their way around online. If an adult doesn't know the pitfalls they can't protect them. Even some four-year-olds have more IT knowledge than a relative who doesn't engage in the online world.

Our school advises parents about online safety through sharing resources and materials on our website, speaking to parents individually to offer advice, sharing information in newsletters and signposting parents to support.

Cyber Security for Safeguarding in Early Years

We are increasingly reliant upon technology for the efficient management of the school. 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. These records are confidential and protected.

Cybercriminals can damage a business, cause a temporary shutdown, expose confidential information and access finances. The reputational damage could be huge and could lead to an investigation by the Information Commissioner's Office, resulting in hefty fines.

We safeguard our school from cybercrime by:

- Backing up all information on the cloud or USB, with password protection.
- Using strong passwords to control access to relevant documents and information on all devices, including folders on computers.
- Ensuring that only the people authorised can access information, and when sending information to parents or professionals, set up a password system so only they can open it.
- Ensuring all devices have protective software from viruses and malware and keep them up to date.
- Knowing how to recognise and deal with suspicious messages or contact.
- Being knowledgeable about legislation and requirements.
- Knowing where to go for advice and how to deal with breaches.
- Ensuring that cyber security is included in your overall online safety policies
- Reviewing and monitoring our safeguards through cyber risk assessments.

Policy Approved: November 2024
Policy Review: November 2025