Online Safety Policy

Millfield is aware of the growth of internet use 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.

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 Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Liz Miller or Deputy DSLs Amber Barlow/Abi Lord**

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; for example pornography, fake news, racist or radical and extremist views***
- ✓ ***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***
- ✓ ***conduct: personal online behaviour that increases the likelihood of, or causes, harm" for example making, sending and receiving explicit images, or online bullying***

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

- We are screen free for the children. We do not use a parent app so have no need for tablets.
- Ensuring the children never use the internet while at Millfield
- Ensure management monitor all internet activities in the setting
- Staff have their own computer in the nursery for accessing Twinkl and programmes to support the curriculum, using word and other programmes to support planning and curriculum activities. Staff have access to the nursery policies and procedures.
- 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
- Staff model safe practice when using any technology with children and ensuring all staff abide by an acceptable use policy; instructing staff to use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated.
- Ensuring no social media or messaging apps are installed on nursery devices
- Use only the nursery camera for taking photographs of the children
- Not permitting visitors access to the nursery Wi-Fi
- Staff have their own Wi-Fi account from the Millfield router.
- Staff's own personal mobiles and devices are not permitted in the nursery. All remain in the staff room at all times.
- Staff must not friend or communicate with parents on personal devices or social media accounts
- 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 John and Liz Miller
- 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 address and telephone number. This is to protect staff, children and parents

If any concerns arise relating to online safety, then we will follow our safeguarding 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
- 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 and are signposted to appropriate sources of support regarding online safety at home which fully supports them to understand how to report an online safety concern. Website links are provided on how to set up filters on their home internet to help prevent age inappropriate content being accessed on devices in their home:
  https://saferinternet.org.uk/guide-and-resource/parental-controls-offered-by-your-home-internet-provider
  https://www.childnet.com/resources/smartie-the-penguin/
- 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.

Policy Reviewed
November 2026