LITTLE GRANGE
NURSERY

ONLINE SAFETY POLICY

At Little Grange Nursery 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.

ASSOCIATED POLICIES

Mobile Phone, Cameras and Digital Devices Policy

Safeguarding and Child Protection Policy

Code of Conduct

Rugby School Group Online Safety Policy

Rugby School Group Data Protection Policy

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:

1. ***Content:*** *being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views*
2. ***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*
3. ***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:

- 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
- 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 and /or photograph children in the setting
- Ensuring that staff do not to use personal electronic devices with imaging and sharing capabilities, including mobile phones, smart watches and cameras

- Never emailing personal or financial information
- 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)
- 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) discussing with the children what they would do if someone they did not know tried to contact them
- 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 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)
- 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
- 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 is posted online, both professionally and personally. This is continually monitored by the setting's management
- 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 and telephone numbers. This is to protect staff, children and parents
- Signposting parents to appropriate sources of support regarding online safety at home.

IT Director/IT Services Department will ensure:

- that the nurseries technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the networks and devices through a properly enforced password protection policy
- that filtering and monitoring is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in School policies.

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 Designated Safeguarding Lead is ultimately responsible for online safety concerns and all concerns need to be raised as soon as possible.

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 via articles posted on Famly

- 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.

Review Date: August 2025

Person Responsible: Anna Biddlestone