

Internet Safety Policy

The use of technology and the internet is a fundamental part of modern life. ICT is delivered in our nurseries and schools as part of the curriculum to teach children skills that they will require growing up in a modern world. As a childcare service, we also have a responsibility to help children to learn about technology and how it can be used to support education and enhance our lives.

Staff provide regular opportunities within the setting for children to explore technology, for example through the use of interactive or programmable toys and various electronic devices including a laptop, iPad and television and gaming consoles. The internet is also an incredible resource for children, for example, to assist with homework, play educational games, research interests / hobbies or chat with friends through social networking sites. The internet can however also be a very dangerous place for children. Some of these dangers include:

- Gaining access to illegal, harmful or inappropriate images or other content.
- Being exposed to harassment and bullying
- Accidentally sharing personal / financial information
- Being vulnerable to online grooming by paedophiles.

We have an obligation to all service users to ensure that they are safe and are protected from potential harm. we do this by:

- Keeping up to date with guidance and advice to safeguard both children and adults online including [Safeguarding children and protecting professionals in early years settings: online safety considerations / Education for a Connected World](#)
- Ensuring children have safe access to the internet by maintaining security system/s, filters and virus protection software on all devices.
- Supervising children at all times when using the laptop or iPad so staff can check which websites they are visiting and what they are doing.
- Talking to the children about what websites they are using and not allowing children access to chat rooms whilst in our care.
- Discussing the importance of keeping safe online with the children for example, not talking to people they don't know or not giving out personal information that could enable people to identify them and never to arrange to meet anyone they have spoken to online.
- Regularly checking search history.
- Limiting the time children spend on computers and ensuring that they spend a balance of time engaged in ICT and other activities.

If you would rather your child was not allowed access to the internet then please let a staff member know.

Data Protection

As staff also use a business laptop and iPad for recording and storing information about children and families (for example care plans, attendance, payment, development records, etc.), we must also consider our responsibilities with regards to data protection. As some of this information may be sensitive, I must be extremely careful as to who can access this data and prevent it from being inappropriately shared. In addition to supervising children at all times, staff also make use of parental controls and multiple user settings to prevent children from accessing inappropriate content or personal files.

Please refer to the **Confidentiality, Privacy and Data Retention Policy** for further information about the data protection procedures and responsibilities.

Emma's Explorers

Date: 05 2025

Review Date: 05 2025