Finch Nest Preschool

Acceptable Use Policy

Date: November 2025

Review: November 2027

Policy intention

This policy outlines the roles and responsibilities of all individuals who have access to and are users of work-related technology systems.

It is important the children learn about the world around them and can keep themselves safe whilst using technology on and offline. We safeguard children by promoting the appropriate and acceptable use of technology within the setting so that they build on their experiences, access and value technology and will be safe in the virtual world.

We ensure all users of technology have an awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Procedure

The technology used at Finch Nest Preschool is listed and numbered and identified if it can be connected to the Wi-Fi or not, on our Asset Register. This includes computers, mobile phones, landlines, photocopiers, laptops, tablets, iPads, Internet, email, CCTV, walkie talkies, wearable technology, message functions on apps, social networking sites, smart watches, cameras, and any other technological devices. The designated safeguarding lead is responsible for all aspects of online safety.

- We help children to develop skills and competencies and have opportunities to understand the world of technology.
- We ensure their virtual environment allows them to communicate and collaborate, promote research and investigation, and provide challenge through problem solving and decision making whilst being safe online, taking care of equipment and developing basic technology skills.
- Our staff understand their safeguarding responsibility when using technology to share information about a child or family, including the use of online journals or apps.
- Our settling in procedures take account of technology used by the child within the home and we provide online safety information to help parents/carers make an informed choice.
- Robust filters and monitoring systems are in place to protect staff and children from potentially harmful online material including terrorist and extremist material.
- Any technology that is removed from our setting is the responsibility of the person who signed the item out and is password protected. Systems are in place to check and sign the item back in.
- Our Wi-Fi is secure, and password protected.
- All devices/technology are kept securely and in line with data protection requirements.
- All staff are responsible for ensuring the physical safety of children whilst using technology.
- All apps, online tools and websites are regularly checked including search history, privacy, and security.

- Children are clear about when they can use a device, how to keep themselves safe and how to take care of equipment.
- We ensure parents/carers are able to reach the setting via phone at all times, in case of emergencies.
- We use work emails and numbers only to protect staff and children.
- We seek parent permission before taking any photographs of a child to record activities and share their progress.
- Any photographs taken will be stored, used, and deleted in accordance with the Information and Records Policy.
- Photographs of a child are not published on any social networking sites or shared with any other person without permission.
- Parents/carers must not use a mobile phone anywhere on the premises, outside or inside at any time e.g. whilst dropping off and collecting child/children.
- Any visitors to the setting will also be asked not to use their mobile phone.
- Parents/carers are made aware of the safe and proper use of technology they bring into the setting, for example during show rounds, open days, parent meetings, events, and productions.
- We ensure safety of all children in attendance and ensure appropriate access to material when using the internet.
- Staff role model the positive use of technology and are aware of overuse.
- Staff are aware of how to report a problem and to escalate a concern about any item of technology.
- Staff are aware of the action to be taken should technology be used inappropriately as in our Safeguarding Policy.
- Staff are aware that the use of technology can be monitored, and information can be used as part of an investigation.
- Staff do not download, install, access, or search any inappropriate content, facility, or data. In order to comply with the Data Protection Act 2018 and GDPR, the setting is registered with the Information Commissioner's Office as a data controller to allow us to store digital images on an SD card device/computer. Our Registration Number with the Information Commissioner's Office is: **ZB625125**
- If we are concerned about children's safety or welfare online through the use of our technology, we will notify agencies with statutory duty without delay.

Other useful policies:

- Information and Records Policy
- Safeguarding Policy
- Child Protection Policy
- CCTV Policy