Safe Internet Use

Fun Fest recognises that the internet is a useful resource for both staff and children, for the purpose of research and entertainment.

In our Club, we use screen time for the purpose of our activities, adverse weather playtimes and at the end of the day whilst children are awaiting collection from parents and carers. However, it must be used with care to ensure that children are kept safe from exposure to harmful material, in accordance with the **Statutory Framework Safeguarding and Welfare Requirements (2024) and The Prevent Duty.**

The Designated Safeguarding Lead _____,is ultimately responsible for online safety concerns.
The use of technology has become a significant component of many safeguarding issues. The breadth of issues classified within online safety is considerable, but can be categorized 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.*

Safeguarding children and protecting professionals in early years settings: online safety considerations - GOV.UK (www.gov.uk)

Within the Club 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 club mobile devices
- Ensuring all devices are password protected, passwords changed regularly and are not written down
- Monitoring all internet usage across the setting
- Providing secure storage of all Club devices at the end of each day, in the office in a locked filing cabinet

- Ensuring no social media or messaging apps are installed on Club devices
- Using only Club devices to record/photograph children in the setting, which will be kept in the office with a signing in and out sheet which will be checked at close of day on the close checklist.
- Never emailing personal or financial information
- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Teaching children how to stay safe online by following the **Safeguarding Policy** and report any concerns they have by completing the **'Logging a Concern about a Child's Welfare and Safety'** and the **DSL must complete their part of this form,** the **'Correspondence Log'** is to be completed. Staff are encouraged to use the link below for any guidance that they need.
- Ensuring children are supervised when using internet connected devices
- Not permitting staff or visitors to access to the Club Wi-Fi
- Providing training for staff, at least annually, in online safety and understanding how to keep children safe online.
- Staff model safe practice when using technology with children and ensuring all staff abide by an acceptable use policy; (see acceptable IT 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
- 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 the setting's management
- Ensuring all electronic communications between staff and parents is professional and takes place via the official Club 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

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, the member of staff must complete

- the **'logging a concern about child's safety and welfare',** the **DSL must complete their part of this form,** the **correspondence log** is to be completed**.**
- 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.

Cyber Security

This policy should be read in conjunction with your Data protection and Confidentiality Policy*, *Acceptable IT Use Policy and GDPR Privacy statement.

Good cyber security means protecting the personal or sensitive information we hold on children and their families from criminals, in line with the Data Protection Act 2018.

To prevent any attempts of a data breach (information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the NCSC Suspicious Email Reporting Service at report@phishing.gov.uk

Useful links for Parents and staff

Online Safety for Children - Tips & Guides | NSPCC
Resource Library (thinkuknow.co.uk)
Safeguarding children and protecting professionals in early years settings: online safety considerations - GOV.UK (www.gov.uk)

online safety briefing for staff

https://moodle.ndna.org.uk/

This policy was adopted on	Signed on behalf of the club	Date for review
10/06/2024	Tina Iezekil	10/06/2025

Written in accordance with the Statutory Framework for the Early Years Foundation Stage (2024): Safeguarding and Welfare Requirements: Safeguarding [3.4 – 3.9].