Online Safety Policy

Our setting is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers and strives to support children, staff and families in using the internet safely.

We refer to 'Safeguarding children and protecting professionals in early years settings: online safety considerations' to support this policy.

Safeguarding children and protecting professionals in early years settings: online safety considerations for managers - GOV.UK

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to line manager/s or the DSL.

Introduction

The use of technology has become a significant component of many safeguarding issues; Child sexual exploitation, radicalisation, sexual predation, cyberbullying. Technology often provides the platform that facilitates harm.

The range of issues classified within online safety is considerable, but can be categorized into four areas of risk:

Content (what they may see)

Being exposed to illegal, inappropriate or harmful videos, pictures or messages - for example, pornography, fake news, racist or radical and extremist views. They may search for it or stumble upon it by accident. Children may need help to consider the reliability of online material.

Contact (who might communicate with them)

Being abused online (including sexually) by people they don't know when gaming or using video chat. Inadvertently sharing their location. Subjected to harmful online interaction with other users - for example, adults posing as children or young adults.

Conduct (how people might behave)

Personal online behaviour that increases the likelihood of, or causes, harm - for example, making, sending and receiving explicit images, or online bullying. Or they may put themselves at risk by sharing too much.

Commerce (how they might be exploited by business)

Risks such as online gambling, inappropriate advertising, phishing and financial scams. They may inadvertently give apps or websites permission to share their location or other personal information, or spend real money via apps or in-game purchases - for example, commercial advertising.

Why Use the Internet?

The Internet is an essential resource to support teaching and learning, therefore it is important for children to learn to be safe online from an early age; our setting can play a part in this process.

Digital skills are vital to accessing life-long learning and employment. Children will use the internet outside of the setting and need to learn how to keep safe online. Staff have a responsibility to help children stay safe online both in and outside of the setting.

How we use the Internet to enhance learning

Internet access is planned to enrich and extend children's learning activities. Staff will help guide the children with online activities to support the learning outcomes for their stage of development.

How children will be using the ICT equipment

Children may be confronted with inappropriate materials, despite all attempts at filtering the internet. Staff will oversee children to ensure they can see any electronic device's screen so that they can intervene when necessary.

How staff will support children to understand the online risks they may face

Staff will work with children to develop an understanding of the online risks they may face, discuss and provide tools, strategies and information to the children (or signpost them to where to get it) and also to their parents/ carers.

The setting will develop/adopt key online safety messages to support this work.

How staff use the internet

The internet is also used in the setting to support the professional work of

staff, to allow effective planning and to enhance the setting's management information and business administration systems.

How will filtering and monitoring be managed

The setting's DSL, in conjunction with (Mikael Georgelin), will ensure that appropriate filters are applied to the electronic devices used by staff and children. They will also review/monitor the sites accessed on a regular basis. The following will be checked as part of an audit of all digital devices used.

- Internet provider filtering system (business level)
- Operating systems controls
- Device safety settings
- Programme safety settings
- Internet security and virus protection

Children's electronic devices in the setting will have parental controls as well as internet security and virus protection. This will reduce children accessing sites of unsuitable content when using the electronic device. Anything that appears unsuitable or offensive will be brought to the manager's/DSL's attention, which will then trigger appropriate action and be recorded as an incident.

All sites that children have access to, will be used and viewed by staff before the children access them and they will be age appropriate and relevant to their learning. Staff will monitor the websites being used by the children during sessions and guide its use. If staff or children discover unsuitable sites have been accessed on the setting's electronic devices, they must be recorded and reported to the DSL immediately so that filters can be reviewed, and appropriate action taken.

The DSL is the lead for reporting online incidents and they will work with the Online Safety Lead overseeing internet use, training staff and developing online safety strategies for children and parents.

Our management will ensure there is sufficient funding and time made available for staff training to use systems.
The setting will seek guidance from expert agencies to ensure safety arrangements are kept up to date:

UK Safer Internet Centre
South West Grid for Learning – Early Years Toolkit

Helping children keep safe online

Staff have a responsibility to help children stay safe online, both in and outside of the setting. There are 4 main areas of risk to

consider: content, contact, conduct and commerce. We will focus on:

• Supporting children to develop their understanding of the online risks they may
face.
• How to prevent or reduce risks.
• How and where to get help and support.
The setting will develop an online safety strategy for children and their parents and
carers, taking these factors into consideration.

Children's mobile phones/devices

It can be assumed that children attending the kindergarten aged 2-5 years old will not bring devices into the setting. The same applies to holiday children. However, if employees discover a device, while they are at the setting children will be required to leave their mobile phones/devices in their bag.

Parents/carers will be informed that children's phones/devices are not allowed on site premises due to the risks involved.

Staff will signpost parents to information on how to set up, filter and control their child's device to reduce the risk of them accessing harmful online material.

Parents and online safety

Parent's attention will be drawn to the settings Online Safety Policy. We will do this by sharing it via permissions on Famly and on our website.

While on the premises parents/carers will be asked to comply with the setting's mobile phones/digital devices and online safety rules. Parents accessing their child's personal online learning journal accounts from home will use their personal emails and passwords that have been set up by the manager/setting.

Staff

Managing content and Information systems

It is important to review the security of the whole ICT system to keep everyone safe.

All ICT equipment is audited and checked at the beginning of each academic year and thereafter is checked regularly.

Staff are responsible for ensuring that material accessed by children is appropriate and for ensuring that the use of any internet derived materials by staff or by children

complies with copyright law.

The point of contact on the setting's website should be the setting address, setting e-mail and telephone number. Staff or children's home information will not be published.

Website photographs that include children will be selected carefully and with permission of the patents. Children's full names will not be used anywhere online, particularly in association with photographs.

Written permission from parents or carers for featuring their child on the website is requested when each child starts at the setting and parents/carers wishes are followed. Parents may change this consent at any time by contacting the setting.

Communication

Managing email

Email is a useful way to communicate with parents about current activities and events in the setting.
The setting's main email login details are known to the manager and deputy manager; they are not shared with other members of staff to ensure confidentiality.
Staff using email will use a setting/ professional email address.

All emails sent to parents are via the setting's/professional email address/es and never from a private/personal email address. When sending emails' all email addresses are kept private. When sending out bulk emails to parents, the email addresses of other parents will never be displayed.

The setting's email addresses must not be used for personal email. Children will not have access to email.

Staff use of the setting's electronic devices

Staff will not use the setting's electronic devices for personal use. The setting will ensure that all programs used and websites accessed are appropriate and that children are not able to access or download material which is unsuitable.

All setting files that contain personal data will be stored appropriately and securely, e.g.: password protected or locked away.

Staff will not forward any of the setting's work, files, information etc stored on the setting's electronic devices to their personal electronic devices, unless this has been agreed and recorded by management as necessary. Any work taken home will be protected as if it were in the setting and open to scrutiny by management.

Staff will not use any personal memory devices in the setting's electronic devices. Memory sticks provided by the setting will be used for work purposes only and will be kept securely.
Generally, all ICT equipment should remain in the setting. This is to minimise the risk of computer viruses and for data protection purposes.

Staff will not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
All email communication will be appropriate and written in a professional manner.

Illegal or inappropriate materials MUST NOT be uploaded, downloaded or accessed.

Staff will ensure that setting's electronic devices are used appropriately to avoid disabling or damaging equipment.

Online learning diaries will be accessed and completed in line with the settings "Acceptable Usage Agreement" procedure.

Social Networking/Media Sites

Social networking sites (e.g.: Facebook, Twitter and Instagram) can be a useful advertising tool for settings and can often be an effective way of engaging with parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such Sites.

Staff, volunteers, students or management must not put details of their work on any form of social networking site.

To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.

No staff are permitted to 'friend' parents/carers currently accessing the setting. New staff starting with the setting may be asked to defriend these people. A safeguarding message is available on request explaining the reason for defriending if required. Or staff will declare any pre-existing friendships with parents/carers to the manager and commit to keeping strict work /life boundaries.
Staff, volunteers, students or management must not engage in any on-line activity that may compromise their professional responsibilities.
Staff, volunteers, students or management must be very cautious about the content they post online. Everyone in the setting must

be mindful that once content is placed online, even if swiftly removed, can remain out in the ether accessible to all.

All staff, volunteers, students and management are to adapt their privacy settings to ensure that only friends can see their personal social networking profiles. In the case of social media sites where you cannot control who sees the content please see point above. Photographs, names of, or comments about children within the setting must never be placed on any social networking site.
All staff, volunteers, students and management must not correspond with the setting's children/families through social networking sites.

Staff will not discuss individual children or their setting on any social networking site. Staff should be aware of possible professional implications/risks when entering any personal details on any gaming or social networking sites (e.g.: YouTube, Facebook, twitter etc).

Staff should be aware that potential employers may conduct online/social media searches when recruiting.
Staff will not be permitted to use the setting's electronic devices to access social networking sites at any time, including designated breaks.

All communications in the setting will be transparent and open to scrutiny. If staff or children discover unsuitable sites, the URL (address) and content must be reported to the manager or named Online Safety Lead. This will be recorded.

All staff must be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.

Handling Complaints

Any complaints about the appropriate use of the internet or other technologies will be handled through the setting's complaints procedure.

Named lead for Online Safety and DSL

Brislington : Ella Ives

Stapleton : Pilar Fernández De La Vega

This policy was adopted by: Out There Forest School and Kindergarten	**Date:** **June 2022**
Reviewed: **July 2023** **To be reviewed:** July 2024	**Signed:** **Jenny Brough**

Further Information

Safeguarding children and protecting professionals in early years settings: online safety considerations

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

Safeguarding children and protecting professionals in early years settings: online safety guidance for practitioners - GOV.UK (www.gov.uk)
South West Child Protection Procedures – provide detailed online information on all aspects of child protection :Online Safety (proceduresonline.com)

Data Protection – Information Commissioners Office, detailed information on all aspects of data protection: https://ico.org.uk/

Internet Matters – Helping parents keep their children safe online: www.internetmatters.org

Common Sense Media - reviews information and age ratings on all sorts of media: https://www.commonsensemedia.org/

South West Grid for Learning
Early Years Resources | SWGfL

UK Safer Internet Centre – Advice and Report Harmful Content Centre
https://www.saferinternet.org.uk/

POSH (Professionals Online Safety Hotline)
https://www.saferinternet.org.uk/

our-
helplines Monday to Friday 10:00am – 4:00pm
For help and support, please email helpline@saferinternet.org.uk
Internet Watch Foundation – To report images of child sexual abuse - Eliminating Child Sexual Abuse Online – Internet Watch Foundation (iwf.org.uk)