



Online use and Safety Policy

Policy statement

We are aware of the growth of internet use and the advantages this can bring. However, we are also aware of the dangers and strive 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.

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 and 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 for children:

The emerging threat of misuse of AI tools to generate intimate images or commit fraud needs consideration in relation to all 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, misinformation, disinformation, conspiracy theories, 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; we 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. Screen use in will be limited, carefully planned and clearly linked to intended learning aims. Staff will help guide the children with online activities to support the learning outcomes for their stage of development.

Early Years

Children will have adult engagement when they access or use screens alone or with other children. It is important to view screens with children to protect them from harmful content and to support their development.

All digital content should be:

- checked to ensure it is suitable for early years children, prior to showing it to the children
- slow-paced, repetitive and predictable - you should therefore avoid fast-paced, over-stimulating content
- advert-free, as young children cannot discern between advertisements and other content
- free of scrolling and autoplay features, to ensure children are not inadvertently exposed to inappropriate content

Apps, software and tools will be assessed by the team for educational, high-quality content designed for children.

Screens will not replace high-quality educator-child interactions, as direct human interaction provides a much richer experience for children.

Consider adopting these practical tools to help online use remain safe and meaningful for children.

Practical tips to follow:

- do not allow children to view screens in a passive or sedentary way, without any interaction or communication from educators
- only use screens with children for short periods at a time, to protect children's ability to focus and concentrate
- screen-free zones: consider designating certain spaces in your setting as permanently screen-free to protect social interaction and learning
- avoid using screens with children during mealtimes or within an hour of a sleep period, as this could affect their sleep quality
- don't have screens on in the background, as they can distract from activities such as social interaction and active play



- avoid using screens for routine management or to calm children, as this impacts on children's ability to learn to self-regulate - screens should also not be used to occupy children (including during periods of transition throughout the day) or manage their behaviour

Screen time advice for children aged 0-5

- b. under 2 years - avoid screen time/use altogether other than in exceptional circumstances such as a video call with parents and carers
- c. 2-5 years - screen time/use should be limited to 1 hour a day, less if possible

We will discuss screen time/use with parents and carers as a child may already reach these screen time limits at home.

Meeting Needs

Some children with SEND or English as an additional language may need a more individual approach when it comes to screen use. Including children with communication challenges which may or may not be diagnosed. Screen-based assistive technology can be an important tool to help these children and families communicate, take part in everyday activities, and create an inclusive learning environment. We will use our professional judgement to determine whether assistive technologies will support children's learning on a case-by-case basis and discuss these with the parent/carers.

How children will be using the ICT equipment

Children may be confronted with inappropriate materials, despite all attempts at filtering the internet. Staff will engage/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, as they get older they will discuss and provide tools, strategies and information to the children (or signpost them to where to get it) and also to their parents/ carers. We will develop/adopt key online safety messages to support this work.

How staff use the internet

The internet is also used by us to support the professional work of staff, to allow effective planning and to enhance our management of information and business administration systems.

1. How will filtering and monitoring be managed?

- Our DSL, in conjunction with staff/committee/management/Online Safety Lead, will ensure that the appropriate filters are applied to our electronic devices and 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. We will consider using Schools and Colleges cybersecurity standards, or the South West Grid for Learning Early Years services or the National Cyber Security Centre for Early Years Guidance to help us reduce risks related to a cyber incident.
- Internet provider filtering system (business level?)
- Operating systems controls
- Back up of important information
- Device safety settings
- Programme safety settings



- Passwords
- Internet security and virus protection
- Children's electronic devices used will have parental controls as well as internet security and virus protection. This will reduce children accessing sites of an 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 our 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.
- We 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
 - National Cyber Security Centre

2. 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.

We will develop an online safety strategy for children and their parent/carers, taking these factors into consideration.

3. Children's mobile phones/devices

- While they are here, 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 covered by our insurance policy.
- 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.



4. Parent/Carers and online safety

- While on the premises parents/carers will be asked to comply with our mobile phones/digital devices and online safety rules.
- Parent/carers 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.
- We will discuss guidance around screen time with parents signposting them to: [Baby and toddler screen time guidance - Best Start in Life](#) or other good quality guidance.

Staff

5. 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 our website will be our address, our 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 will not allow individual children to be clearly identified. The emerging threat of misuse of AI tools to generate intimate images of children will be carefully considered. 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 with us and parents/carers wishes are followed. Parents may change this consent at any time by contacting us directly.

6. Communication

Managing email: Email is a useful way to communicate with parent/carers about our current activities and events.

- Our 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 our/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.
- Our email addresses must not be used for personal email.
- Children will not have access to email.

7. Staff use of the setting's electronic devices

- Staff will not use our electronic devices for personal use.
- We 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 of our files that contain personal data will be stored appropriately and securely, e.g.: password protected or locked away.
- Staff will not forward any of our work, files, information etc stored on our 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 our electronic devices. Memory sticks provided by us will be used for work purposes only and will be kept securely.
- Generally, all ICT equipment should remain here. 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 our electronic devices are used appropriately to avoid disabling or damaging equipment.
- Online learning diaries will be accessed and completed in line with our **"Use of online learning diary system and technological devices by staff" procedure.**

8. Social Networking/Media Sites

Social networking sites (e.g.: Facebook, Instagram, What's App) can be a useful advertising tool for us 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 our page.
- 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 working for us (including volunteers) 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 that attend must never be placed on any social networking site.
- All staff, volunteers, students and management must not correspond with the our children/families through social networking sites.
- Staff will not discuss individual children or their workplace 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, Instagram etc).
- Staff should be aware that potential employers may conduct online/social media searches when recruiting.
- Staff will not be permitted to use our 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 and DSL. 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.

9. Games Consoles

- Staff will ensure that all games consoles and games used are suitable and appropriate for the developmental stages of children in their care.
- Use of games consoles will be supervised, monitored and children encouraged to participate in a broad range of activities.
- All games used should be originals and not copies.
- Parents/carers should be made aware that computer games are available and have the option to request that their child does not access this equipment.
- Children should be closely supervised to ensure that they are not accessing the Internet via the console. Or, if they are permitted to do so that the websites accessed are appropriate and we have put in place appropriate safeguards.

10. GDPR

Horfield Welly Pre-school understands that we have a duty to comply with the UK-General Data Protection Regulations (UK-GDPR). To do this we will research our responsibilities

(<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>) and fulfill them according to the type and size of our organisation.

The Information Commissioner's Office has condensed the Data Protection Principles into six definitions, which are referred to as the Privacy Principles. They are:

1. You must have a lawful reason for collecting and processing personal data and must do it in a fair and transparent way. There are six lawful reasons for doing this – see www.ico.org.uk
2. You must only use the data for the reason it is initially obtained.
3. You must not collect any more data than is necessary.
4. It must be accurate and there must be mechanisms in place to keep it up to date.
5. You cannot keep it any longer than needed.
6. You must protect the personal data.

These privacy principles are supported by a further principle – accountability.

We will endeavour to train all staff on data protection where appropriate and possible.

11. Handling Complaints



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

12. Named lead for Online Safety and DSL: Courtney Haley

Further Information:

[Help for early years providers : Screen use](#)

[Baby and toddler screen time guidance - Best Start in Life](#)

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:

[Welcome to the South West Child Protection Procedures \(trixonline.co.uk\)](#)

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](#)

National Cyber Security Centre

[Early Years practitioners: using cyber security to protect... - NCSC.GOV.UK](#)

Cyber security standards for schools and colleges

[Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK](#)

UK Safer Internet Centre – Advice and Report Harmful Content Centre

<https://www.saferinternet.org.uk/>

POSH (Professionals Online Safety Hotline) [Professionals Online Safety Helpline - UK](#)

[Safer Internet Centre](#) 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 \(iwf.org.uk\)](#)