E-Safety Policy

The Internet is an accessible tool for children in Early Years settings: gaming, learning apps, etc.

At HPPN we have a duty to ensure that children are protected from potential harm both within and beyond the learning environment. Every effort will be made to safeguard against all risks; however, it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

This policy applies to all staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above-mentioned groups, such as mobile phones or iPads / tablets which are brought into HPPN. This policy is also applicable where staff or individuals have been provided with devices issued by the setting for use off-site, such as a work laptop, iPad, or mobile phone.

Staff responsibilities:

Practitioners (including volunteers)

At HPPN all staff have a shared responsibility to ensure that children under our care are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

A copy of this policy is issued to all staff and shared with volunteers and students.

Parents and practitioners should encourage children to type in the code to open the inner gate as it embeds the principle of using a password to unlock the door. This prepares them for using passwords on computers and other devices.

ICT Team:

We have contracted support from 4TC for our ICT needs. Our regular ICT Technician is Adam Forton.

The ICT Technician is responsible for ensuring that:

- The setting's ICT infrastructure is secure and not open to misuse or malicious attack.
- Anti-virus software is installed and maintained on all setting machines and portable devices.

- The setting's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the Designated Person for Safeguarding.
- Any problems or faults relating to filtering are reported to the Designated Person for Safeguarding and to the broadband provider immediately and recorded on the e-Safety Incident Log.
- Users may only access the setting's network through a rigorously enforced. password protection policy.
- He/she keeps up to date with e-safety technical information in order to maintain the security of the network and safeguard children.
- The use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the Designated Person for Safeguarding.

Broadband and Age-Appropriate Filtering:

Broadband provision is essential to the running of HPPN, not only allowing for communication with parents and carers, but also providing access to a wealth of resources and support. At HPPN we use internet enabled devices, including iPad educational apps and games, to enhance the learning experiences of children and as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available.

It is the responsibility of the Manager (who is also the Designated Safeguarding Person) to ensure that HPPN's internet provision is as safe and secure as is reasonably possible.

- Filtering levels are managed and monitored on behalf of the setting by our ICT support team.
- Age-appropriate content filtering is in place across the setting, ensuring that. staff and children receive different levels of filtered internet access in line with user requirements (e.g., YouTube at staff level but blocked to children).
- Online safety concerns must be reported to the Designated Safeguarding Person who will record concerns, take appropriate actions, and record those. actions.

Use of email:

- At HPPN we provide all staff with access to a professional email account to use for all work-related business, including communication with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- All electronic communications between staff and parents should be professional and take place via the official nursery communication channels, e.g., the setting's email addresses and telephone numbers.
- All emails should be professional in tone and checked carefully before sending.

Use of Mobile Phones

At Holland Park Pre-Prep & Nursery (HPPN), we promote the safety and welfare of all children in our care. We believe our staff should be completely attentive during their hours of working to ensure all children in the nursery receive good quality care and education. To ensure the safety and well-being of children we do not allow staff and visitors to use personal mobile phones whilst working in the classroom.

Staff must adhere to the following:

- Mobile phones/smartwatches/fitness watches are either turned off or on silent and not accessed during your working hours.
- During hours at work Mobile phones/smartwatches/fitness watches should not be stored outside of the main classroom. Devices should be stored in the locked device box in the printing room.
- Mobile phones/smartwatches/fitness watches can only be used on a designated break and then this must be away from the children.
- Mobile phones/smartwatches/fitness watches should be stored safely and not be used whilst working in the classroom with children present.
- During outings, staff will use mobile phones belonging to the nursery wherever possible. Photographs must not be taken of the children on any personal phones or any other personal information storage device.

Use of Social Networking Sites:

HPPN realise that social media and networking websites have become a regular part of everyday life and that many people enjoy using sites such as Facebook, Instagram, or Twitter. However, we are also aware that these sites can become a negative forum for complaining or gossiping, and care must be taken not to breach our confidentiality policy not to offend anyone when using these services. All staff, students, and volunteers, whether current or past, agree to abide by this policy.

The following policy has been designed to give staff clear guidelines as to what HPPN expect of them when accessing these sites. The absence of, or lack of, explicit reference to a specific website or service does not limit the extent of the application of this policy. Where no policy or guidelines exist, employees should use their professional judgment and take the most prudent action possible. Individual members of staff should consult with their manager or supervisor if uncertain.

Guidance for Personal Use:

If you have your own personal profile on a social media website, you should make sure that others cannot access any content, media, or information from that profile that.

(a) you are not happy them to have access to; and

(b) which would undermine your position as a professional, trusted, and responsible person.

As a basic rule, if you are not happy for others you work with to see particular comments, media or information, simply do not post it in a public forum online.

When using social media sites, staff members should consider the following:

- Setting your privacy settings on your profile so that only people you have accepted as friends can see your content.
- You must not post comments about work, anyone associated with work or name the setting you work at.
- Reviewing who is on your 'friends list' on your personal profile. In most situations you MUST not accept friend requests on your personal profile from 'clients' you work with (this includes parents etc.)
- You MUST not direct message any 'clients' or their relatives. If parents contact, you inform a member of the senior leadership team.
- Ensuring personal blogs and social networking accounts have clear disclaimers that the views expressed by the author are theirs alone.
- Ensuring information published on the internet complies with HPPN's confidentiality and data protection policies. Breach of confidentiality will result in disciplinary action and may result in termination of your contract.
- Ensuring you are always respectful towards: HPPN, other staff members, parents, and families (including children and other relatives) or other agencies and partners. Staff should be aware that any disrespectful comments to the above might be seen as libellous and could result in disciplinary action or termination of your contract.
- HPPN logos and trademarks may not be used without written consent.
- Any employee who becomes aware of social networking activity that would be deemed distasteful should make the Manager aware as soon as possible.

All staff using official accounts must adhere to the above guidelines; breach of this policy may result in disciplinary action or termination of your contract.

Parents and visitors' use of social networking

We promote the safety and welfare of all staff and children and therefore ask parents and visitors not to post, publicly or privately, information about any child on social media sites. We ask all parents and visitors to follow this policy to ensure that information about children, images and information do not fall into the wrong hands.

We ask parents not to:

- Send friend requests to any member of nursery staff.
- Screen shot or share any posts or pictures or information from the nursery this includes updates and pictures from HPPN nursery management software Famly on social media platforms or send them to friends or relatives via messaging apps.
- Post any photographs to social media that have been supplied by the nursery with other children in them (e.g., Christmas concert photographs or photographs from an activity at nursery)

We ask parents to:

- Share any concerns regarding inappropriate use of social media through the official procedures (please refer to the Partnership with Parents' Policy, Complaints Procedures and Grievance Policy).

Photographs and Video:

Refer to Confidentiality and Data Protection Policy within Information and Records Policy.

Digital photographs and videos are an important part of the learning experience in HPPN and as such staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, refer to the Confidentiality and Data Protection Policy.

- Written consent must be obtained from parents or carers before photographs or videos of young people will be taken or used within the setting, including displays, learning journals, the setting's website, or other marketing materials. This is updated on a regular basis to ensure permission still stands.
- We ensure that parents understand that their child's picture may appear in another child's shared picture/learning journal if they are part of the same activity/ experience.
- Parents are informed that we have CCTV in the classroom in the parent handbook and can access is only for management use only. However, this will be waived if an incident occurs and parent requests. This can be authorised at the discretion of management team with a member of the management team present.
- Staff will ensure that children are at ease and comfortable with images and videos being taken.
- Staff must not use personal devices, such as cameras, video equipment or camera phones to take photographs or videos of children. However, in exceptional circumstances were parental and management permission MUST be granted.
- Parents are not permitted to use any recording device or camera (including those on mobile phones or smartwatches) on the nursery premises
- Images and videos taken with HPPN iPads MUST be password protected.

Laptops / iPads / Tablets:

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the ICT team.
- Personal use of the setting's laptops or computing facilities whilst on site is kept to a minimum, only permitted during break times and only in the staff room or office.
- Personal use of school laptops / iPads whilst off site is not permitted.
- All activities carried out on the setting's devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will ensure that the setting's laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring and servicing.
- HPPN-issued devices only should be used for school purposes and, if

containing sensitive information or photographs of children, should not leave the premises unless encrypted or deleted.

- Images and videos taken with HPPN devices must be deleted regularly
- The use of nursery devices; class mobiles, Ipad's and laptops, must only be used for nursery purposes.
- All nursery devices will have red covers so that they are easily identified.
- The nursery devices will not have any social media apps.
- The Manager is ultimately responsible for the security of any data of images held of children within the setting.

Children's Use:

- The use of laptop, iPad, interactive whiteboard and other electronic devices must always be supervised by an adult and any games or apps must be from a pre-approved selection checked and agreed by the Manager and / or Designated Person.
- Online searching and installing or downloading of new programmes and applications is restricted to authorised staff members only. Children are not able to search or install anything on a setting device.
- Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any Apps which record and store children's personal details, attainment or photographs. Only HPPN-issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.

Data Storage and Security:

Sensitive data, photographs and videos of children are not stored on HPPN devices which leave the premises (e.g. laptops, mobile phones, iPads, USB memory sticks etc.) unless encryption software and/or password protection is in place.

Incident Reporting:

All filtering change requests must be recorded by the ICT support team and the Manager. All filtering changes must be authorised by the Manager. Details of ALL e-safety incidents must be recorded by staff encountering them and monitored monthly by the Manager.

Help:

If setting's need to report illegal images (child sexual abuse material), this should be directed to the Internet Watch Foundation (IWF): www.iwf.org.uk

If staff are worried about online abuse or the way that someone has been communicating online, they should contact the Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk/ceop-reporting/

For further information, staff should contact either or both of the UK Safer Internet Centre Helpline for Professionals:

www.saferinternet.org.uk/professionals-online-safety-helpline or the NSPCC:

www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership/

Date:	September 2024
By:	Danny Webb
Review date:	September 2025