Harvard Park Policies and Procedures:

Online Safety (including mobile phones, camera's, tablets and electronic devices with imaging and sharing capabilities)

59. Online Safety (including mobile phones, camera's, tablets and other electronic devices with imaging and sharing capabilities)

Policy Statement

We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

To ensure our online safeguarding practice is in line with statutory requirements and best practice we will access the guidance '*Safeguarding children and protecting professionals in early years settings: online safety considerations'.* Furthermore, we will share with our staff the '*Online Safety Guidance for Early years* educator' guidance (please refer to further guidance section).

Harvard Park sees the children's health and safety as of paramount importance. We understand that prolonged use of inactive ICT equipment such as a computer can lead to health problems such as eye strain and obesity, we therefore limit the children's time on this apparatus to 20 minutes. All internet sites will be vetted by staff to ensure their appropriateness before children are able to access them. Harvard Park endeavour to ensure that all resources in the setting are free from any violence and stereotyping. We provide resources with positive images which reflect the diversity of our community.

Procedures

Our designated person (manager) responsible for co-ordinating action taken to protect children is:

Carol Mayell supported by Elvia Acosta– Day Nursery

Victoria Close supported by Jeanna Smith – Pre-School

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and can recognise and manage the risks posed in both the real and the virtual world.

Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies' refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them to access content and communications that could raise issues or pose risks; the issues are:

Content – being exposed to illegal, inappropriate or harmful material.

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm.

I.C.T Equipment

- The setting manager and/or director ensures that all computers have up-to-date virus protection installed.
- Tablets are only used by educators for the purposes of observation, assessment and planning and to take photographs for individual children's learning journals.
- There may be occasions where tablets are used to provide information such as access to the Birth to 5 Matters documentation or other informative platforms. However, this is cleared with Managers prior to being accessed.
- There may be occasions where music playing platforms may be accessed such as YouTube. However, this is cleared with Managers prior to being accessed.
- Staff follow the additional guidance provided with the system.

Internet Access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies)
- When using video sharing sites such as YouTube, children are never left unattended with any devices. When used for musical purposes, the screen is shielded from the children. When used for educational purposes, videos are vetted by the designated safeguarding lead to ensure they are appropriate.
- Children are taught the following stay safe principles in an age-appropriate way:
  - Only go online with a grown up
  - Be kind online and keep information about me safe
  - Only press buttons on the internet to things I understand
  - Tell a grown up if something makes me unhappy on the internet.
- Staff support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All computers for use by children are sited in an area clearly viable to staff and are never left unsupervised, they are also have no internet connection.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at Eliminating Child Sexual Abuse Online | Internet Watch Foundation IWF (www.iwf.org.uk).
- If a second-hand computer, tablet, camera or mobile phone is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it. They will ask the person donating to restore factory settings before donating.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Strategies to minimise risk include

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied – default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise all children closely.
- Role model safe behaviour and privacy awareness. Talk to the children about safe use, for example ask permissions before taking a child's picture even if parental consent has been given.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately (source: Safeguarding children and protecting professionals in early years settings: online safety considerations - GOV.UK)

Personal Mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place i.e. the staff room. The setting manager completes a risk assessment for where they can be used safely.
- During staff use of the day nursery staff room, there is a clear, high-level window between the Baby Studio and the staff room that is only visible when standing. To maintain privacy within the Baby Studio, staff using mobile phones during their personal breaks are required to remain seated, ensuring that phone cameras are not directed towards the Baby Studio.
- During staff use of the pre-school kitchen, there are two clear windows that remain visible at all times. One overlooks the Smallberry Green Playground, and the other provides a view into the main room. To maintain privacy, staff must not take photographs of themselves during working hours (e.g. selfies). Staff should also remain mindful of their positioning and the direction of their mobile devices—such as facing away from windows while using their phones—to ensure that privacy is consistently upheld.
- At Day Nursery, Feltham - Personal mobile phones are put into aeroplane mode, on silent and stored in the secondary office in a slated storage unit.
- At Pre-School, Isleworth - Personal mobile phones are put into aeroplane mode, on silent and stored in the office area, next to computer in a slated storage unit.
- In an emergency, personal mobile phones may be used in the privacy of the office or staff room with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Staff do not take their personal mobile phones on outings.
- Staff do not use personal equipment to take photos of the children.
- Parents/Carers and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their

office periodically throughout the day. Visitors are advised of a private space where they can use their mobile phones.

- Children do not bring mobile phones or other ICT devices with them onto the premises. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in mangers office until the parent collects them at the end of the session.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, of for displays, and are only taken on equipment belonging to the setting. Children are given the opportunity to consent to their photograph being take, even if parent/carer permissions are in place.
- Camera and video use is monitored by the setting manager.
- Where parents/carers request permission to photograph or record their own children at special events, general permission is first gained form all parents/carers for their children to be included. Parents/carers are told they do not have the right to photograph or upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place.
- If photographs are used for publicity, parental/carers consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed with their name on artwork or in a sweatshirt with the name of their setting on it.

It is essential that photographs are taken and stored appropriately to safeguard the children in our care.

- Only the designated Harvard Park cameras, tablets and phones are to be used to take any photos within the setting or on outings. Images taken on these cameras, tablets and/or phones must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress. All staff are responsible for the location of the cameras, tablets and phones; all of which should be placed within the manager's office or for pre-school, the lockable cupboards above the computer.

  Day Nursery: Tablets (9) Phones (3) Pre-School: Tablets (5) Phones (2)

- Images taken on the settings trip phones must be downloaded on site as soon as possible, ideally once the children have returned from their off-site trip by the IT Consultant who is the designated member of staff and kept for Learning Journal purposes for one month. Day Nursery phones are used for outing purposes and emergency calls will off site only. Pre-School have their main line for the setting and then a secondary outing phone which is used only for outing purposes and emergency calls while offsite.

- Under no circumstances must cameras/tablets of any kind be taken into the toilet area or nappy changing area. If photographs need to be taken in the toilet area i.e. photographs of the children washing their hands, then the Designated Safeguarding Lead (DSL) must be asked first and staff to be supervised whilst carrying out this kind of activity. At all times the camera must be placed in a prominent place where it can be seen.
- Under no circumstances are students, volunteers or work experience, allowed to use the cameras/tablets. If they are supervised or taking a picture of a member of staff doing an activity, they must hand over the camera/tablet to a practitioner when the task is complete. At no other point should they come into contact with image capturing technology.

In the event of a camera, tablet and/or being misplaced or lost, a full search of the building and staff fleeces/ yellow coats will be conducted. Early years educators are to try and remember where they last had it and who had it last. If the camera/tablet/phone is not found, a search of staff personal belongings will be conducted. If after these, a phone call to the police will be conducted by Manager in charge for that day. The same procedure will be followed in the case of a missing camera, tablet or memory card. Failure to adhere to the contents of this policy will lead to disciplinary/safeguarding procedures being followed.

Cyber Bullying

If staff become aware that a child or young person is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents/carers and refer them to help, such as: NSPCC – Telephone: **0808 800 5000** or www.nspcc.org.uk or ChildLine – Telephone: **0800 1111** or www.childline.org.uk .

Use of Social Media

Staff are expected to:

- Understand how to manage their security settings to ensure that their information is only available to people they choose to share information with.
- Ensure the organisation is not negatively affected by their actions and do not name the setting.
- Are aware that comments or photograph's online may be accessible to anyone and should use their judgement before posting.
- Are aware that images, such as those on Snapchat may still be accessed by other and a permanent record of them made, for example, by taking a screenshot of the image with a mobile phone.
- Observe confidentiality and refrain from discussing any issues relating to work.
- Not share information they would not want children, parents/carers or colleagues to view.
- Set privacy settings to personal social networking and restrict those who can access.
- Not accept service users/children/parents as friends, as it is a breach of professional conduct.
- Report any concerns or breaches to the designated safeguarding lead in their setting.

- Not engage in personal communication, including on social networking sites, with children and parents/carers with whom they act in a professional capacity. There may be occasions when the educator and family are friendly prior to the child coming into the setting. In this case, information is shared with the manager and designated safeguarding lead and a risk assessment and agreement in relation to boundaries are agreed.
- Staff should be aware of their online conduct and report any issues including online bullying towards them or colleagues. They should be aware that their personal digital profile can impact the setting. Staff should discuss with Designated Safeguarding lead (DSL) if they have pre-existing online friendships or relationships with any family members of the children in their care. This can be managed with appropriate online behaviour guidance on boundaries.

Email

- Children are not permitted to use email in the setting. Parents/carers, volunteers and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Staff send personal information by encrypted email and always share information securely.

Smart watches and other devices which connect to onsite WIFI or mobile networks

- Personal smart watches or other WIFI enabled devices are not used by our staff on the premises during working hours. They are to be put on aeroplane mode as to not receive notifications during working hours.
- Under no circumstances are these allowed to be used for anything other than telling the time within the setting. This includes on outings where children from the premises are present.
- These rules also apply to the visitors or outside agencies supporting staff in other settings.

Electronic learning journals for recording children's progress

- Managers seek permission from the senior management team and parents/carers prior to using any online learning journal for evidence which may need to be provided to an outside agency.
- Staff adhere to the guidance provided with the system at all times. This may be by the setting or the company itself. It is not limited to these two options.
- Under no circumstances are passwords and pin numbers used to access the electronic learning journals outside of working hours.

Use/distribution of inappropriate images

- Staff are aware that is an offense to distribute indecent images and that is it an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the designated safeguarding lead who follows procedure Allegations against staff, volunteers or agency staff.

- Staff are aware that grooming children and young people online is an offence and concerns about a colleague's or others' behaviour are reported (as above).
- We are registered with ICO.

Our designated person responsible for co-ordinating action taken to protect children is:
Amy Saunders and our IT Support - Quantus Ltd - Unique Business Systems Integration Company - QIS Ltd

Further guidance
NSPCC and CEOP Keeping Children Safe Online training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

Safeguarding Children and Protecting Professionals in Early Years Provisions Online Safety Considerations for Managers:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776470/UKCIS_Early_Years_Online_Safety_Considerations_for_Managers.pdf

Safeguarding Children and Protecting Professionals in Early Years Provisions Online Safety Guidance for Early years educator:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776473/UKCIS_Early_Years_Online_Safety_Guidance_for_Early years educator__1_.pdf

Early Years early years educator: using cyber security to protect your provisions:
https://www.ncsc.gov.uk/guidance/early-years-early years educator-using-cyber-security-to-protect-your-provisions

This Policies and Procedures pack was adjusted by Harvard Park.
Date meeting was held on 30/04/2026
Signed on behalf of the Directors and Proprietors
Nicki Saunders and Tracey Milstead