06 Safeguarding children, young people and vulnerable adults procedures

06.9 E-safety (including all electronic devices with internet capacity)

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world. Safeguards include setting clear boundaries - time limiting **online** use and setting up passwords and parental controls to ensure children cannot access inappropriate sites.

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 allows them access to 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

Laptops

- Staff are aware to advise Childcare Manager immediately if virus protection software expires, if unable to update themselves.
- Any staff member issued with a laptop for work purposes or have access to a shared laptop to sign a 'Laptop – Staff Declaration' document.
- Laptops are locked when left unattended and stored securely when not in use.
- Laptops are only removed from the premises (Horns Drove Community Childcare) with the prior permission of the Childcare Manager.
- Staff members are aware that passwords must **NOT** be shared with other staff and are for their own use only.

- USB devices may only be used with the prior consent of the Childcare Manager and must only contain work related information.
- Laptops are used for work related purposes only (not used in breaks for personal use – personal emails/documents/images must not be emailed/downloaded or stored on company equipment).

Tablets

- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Tablets remain on the premises unless prior consent given by Childcare Manager i.e planned off-site outings
- Tablets are stored securely when not in use.
- Tablets are used for work related purposes only (not used in breaks for personal use - personal emails/documents/images must not be emailed/downloaded or stored on company equipment).
- All photographs are deleted from all tablets, minimum at the end of each academic year, by the Childcare Manager.

Printers

- Printers are only used for work related purposes. In an emergency, any personal use must be agreed in advance with the Childcare Manager.
- Staff are aware the use of the printer is regularly monitored.

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

- Personal mobile phones, Smart watches 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 e.g. staff room. The setting manager completes a risk assessment for where they can be used safely.
- Staff members do not access social networking sites such as Facebook, X, Instagram on their personal devices in work time. If used during breaks, it must be away from the floor and refrain from discussing work related content and to be mindful of content accessed and suitability for the workplace.
- During working hours, personal mobile phones are switched off and stored in lockers or a locked office drawer. Smart watches may be worn with notifications disabled.
- In an emergency, personal mobile phones may be used in the privacy of the office with permission of Child Care Manager/Deputy Manager.
- 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 mobile phones on outings (office mobile provided).
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors do not use their mobile phones on the premises, these are stored in the office 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.

Work mobile phone (no internet access/no camera facility)

Horns Drove Community Childcare may provide a mobile phone to enable staff to carry out their work safely, effectively and efficiently.

- All phones should be pre-set with Horns Drove Community Childcare number in case of emergencies.
- Personal (non-business) calls may be made in certain circumstances as long as they are appropriate and kept short. The calls that are permitted are to inform family and friends of a change to work plan, personal crisis, etc.
- Staff are aware that work mobile phone is routinely monitored.
- Loss or theft of the work mobile phone to be reported immediately to the Child Care Manager.

Internet access

- Children never have unsupervised access to the internet.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are used responsibly to ensure content is appropriate. Any access in preparation for learning to be away from sight of the children and staff to ensure content is appropriate prior to use. Staff member to monitor throughout session to ensure any inappropriate content can be removed from sight immediately**.**
- 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 safely
  - 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 visible to staff.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- 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.
- 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 children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Make use of home visits to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety

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, or for displays, and are only taken on equipment belonging to the setting.
- Camera and video use is monitored by the setting manager.
- Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a 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 consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.
- Parental consent is obtained for use of photographs internally on Registration and again annually. Parents/carers are able to update throughout the year on Famly e.g. share on Famly or newsletters.
- Parental consent is obtained for use of photographs externally on Registration and again annually. Parents/carers are able to update throughout the year on Famly e.g. Facebook or Instagram.

Systems

- Staff members are aware that passwords must **NOT** be shared with other staff and are for their own use only.
- Staff are aware if accessing internal systems remotely e.g. Famly, One-Drive etc, Educare etc, this must only be for work-related purposes and approved by Childcare Manager.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 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 in any content or in any settings/profiles e.g. Facebook.
- To be aware that comments or photographs online may be accessible to anyone and should use their judgement before posting.
- To be aware that images, such as those on social media platforms may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone.

- To observe confidentiality and refrain from discussing any issues relating to work.
- To not share information, they would not want children, parents or colleagues to view.
- To set privacy settings to personal social networking and restrict those who can access.
- To report any concerns or breaches to the Childcare Manager – Safeguarding Lead or the Deputy Manager or Director in their absence.
- To not to engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the staff member and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed.
- To ensure Horns Drove Community Childcare 'WhatsApp' group is not used to share personal information on individuals within the setting. Appropriate channels for communication to be used to share personal, confidential information e.g. Famly, communication book, emails or verbally with those concerned.

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern, this is raised with the designated safeguarding lead or deputy (Childcare Manager/Deputy Manager.

All staff read E-Safety Policy and sign declaration to confirm read and understood as part of the initial Induction programme.

Disciplinary action may be taken if there is evidence of a staff member not following the E-Safety Policy.

Document

Date adopted	24th September 2024
Date last reviewed	2nd December 2025
Date to be reviewed	23rd September 2025
Signed	Michelle Overton
Name of signatory	Michelle Overton
Role of signatory	Childcare Manager

Version Log

Version	Changes	Date Adopted	Name
1.00		24th September 2024	Michelle Overton
2.00	Reflect changes in EYA policy – November 2024	2nd December 2024	Michelle Overton