HARPOLE PRE-SCHOOL

"Kind Hands, Kind Hearts, Fun Learning"

1.7 Acceptable Use (AUP) and E Safety Policy
Policy & Procedure

Harpole Pre-school has adopted the Pre-school Learning Alliance (PLA) policy Acceptable Use Policy. The PLA ensure that their policies adhere to statutory guidance and legislative procedure and they provide the pre-school with any updates. All policies and procedures are ratified by the Pre-school Trustees on a rolling programme. The pre-school staff, led by Sharon Matthews, ensure that their practice is in line with the policies and procedures outlined in the PLA guidance.

Aims

- To emphasise the need to educate staff and parents about the pros and cons of using new technologies both within and outside the setting.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or parent, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

1. <u>Roles and responsibilities of the setting:</u>

1.1 *Trustees*

It is the overall responsibility of the manager to ensure that there is an overview of e-Safety (as part of the wider remit of Safeguarding) across the setting.

The manager will ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

The Management Trustees will also ensure the policy is reviewed periodically (bi-annually).

1.2 *Staff or Trustees*

It is the responsibility of all adults within the setting to:

- Ensure that they know who the designated person for Child Protection is within setting, so that any misuse or incidents which involve a child can be reported. Where an allegation is made against a member of staff it should be reported immediately to the Chairperson.
- Be familiar with the Behaviour, Safeguarding and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately.

- Alert the business manager of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Use electronic communications in an appropriate way that does not breach the GDPR (General Data Protection Regulations) 2018.
- Remember confidentiality and not disclose confidential information.
- Ensure that they follow the correct procedure for any data required to be taken from the setting premises.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.

2. <u>Appropriate and Inappropriate Use by staff or adults</u>

All staff should receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules. The Acceptable Use Rules will be displayed in the setting as a reminder that staff members need to safeguard against potential allegations.

In the event of inappropriate use

- If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the chairperson immediately and then the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.
- In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

3. <u>Online Safety</u>

It is important that children and young people attending Harpole Pre-school 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 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

- The manager at Harpole Pre-school ensures that all computers have up-to-date virus protection installed.
- Tablets are only used by educators at Harpole Pre-school for the purposes of observation, assessment, and planning and to take photographs for individual children’s learning journeys.
- Tablets remain on the premises and are always stored securely when not in use.
- Staff follow the additional guidance provided with the system.

Internet access

- Children never have access to the internet within the setting.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- 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 at Harpole Pre-school 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.
- 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 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-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners

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

- Personal mobile phones and internet enabled devices are not used by staff at Harpole Pre-school during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place, for example the staff room.
- Personal mobile phones are stored in a safe place away from the children and daily activities.
- In an emergency, personal mobile phones may be used in private 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 mobile phones on outings.
- Members of staff do not use personal equipment to take photographs of 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, but phones should still be stored away from any areas that children access and the setting phone number given to visitors so that they are still contactable. Visitors are advised of a private space where they can use their mobile.

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, for example to record learning and development or for displays, and are only taken on equipment belonging to the setting. Children are given the opportunity to consent to their photograph being taken, 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 from all parents/carers 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, for example children may be identified if photographed in a sweatshirt with the name of their setting on it.

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 Harpole Pre-school is not negatively affected by their actions and do not name the setting
- be aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- be aware that images, such as those on Snapshot 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
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to 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 with whom they act in a professional capacity. There may be occasions when the educator 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

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 that a colleague at Harpole Pre-school is behaving inappropriately, staff advise the designated safeguarding lead who follows procedure 1.12 Allegations against staff, volunteers or agency staff.

This policy was adopted by	Harpole Pre-school	*(Name of provider)*
On		*(date)*
Date to be reviewed		*(date)*
Signed on behalf of the provider		
Name of signatory		
Role of signatory		

Appendix A

Policy statement

What is an AUP (Acceptable Use Policy)?
An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within an educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by people in both home and educational environments include:

- Websites
- Social Networking and Chat Rooms
- Gaming
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Video Broadcasting

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. The policy should also provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It explains procedures for any unacceptable use of these technologies by adults and children.

Why have an AUP?
The use of the internet as a tool to develop learning and understanding has become an integral part of life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst these technologies are accessed.

It is also important that adults are clear about the procedures, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst the setting should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children continue to be protected.