



HARPOLE PRE-SCHOOL

"Kind Hands, Kind Hearts, Fun

1.7 Acceptable Use Policy (AUP) Policy & Procedure

Harpole Preschool has adopted the Preschool Learning Alliance (PLA) policy Acceptable Use Policy. The PLA ensure that their policies adhere to statutory guidance and legislative procedure and they provide the preschool with any updates. All policies and procedures are ratified by the Preschool Trustees on a rolling programme. The preschool 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. Roles and responsibilities of the setting:

1.1 *Trustees*

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

The Business 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 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. Appropriate and Inappropriate Use by staff or adults

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. Technological Tools & Equipment

3.1 *Mobile phones and other emerging technologies*

- The setting does allow staff to bring in personal mobile phones or devices. However mobile phones should not be used in session and can only be used in case of emergencies at the discretion of the Pre-School Manager.
- All personal mobile phones from staff are stored in one central place at the start of the working day.
- When visitors arrive during the session, once the visitors log has been signed they are requested to either store their mobile phone with the others or put it away in their bag.
- Parents and visitors are requested not to use their mobile phones whilst on the premises. We make an exception if it is an emergency or a visitor's company operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where there are no children present.
- In specific circumstances where a professional comes into the Pre-school to support the group with additional activities e.g. music they can use their phone for music in the presence of another member of staff but must not take photos or use their phone for anything else.
- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- We reserve the right to check visitors' mobile phones on leaving the building to ensure no images have been taken.

- If our members of staff or volunteers take their own mobile phones on outings, for use in the case of an emergency, they must not make or receive personal calls as this will distract them.
- The setting is not responsible for any theft, loss or damage of any personal mobile device.

3.2 Video Cameras and Cameras

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in the setting there is access to:

- Video Camera
 - Digital cameras
- The use of camera and video cameras is to be used by staff to support children's development and engage parents in children's learning through photographs and recordings which demonstrate activities and achievements. The setting may also use photographic and video images in the use of marketing the pre-school.
 - Once photographs have been printed, the images are stored on a secure USB port for use during the current academic year, at the end of the year the photographs are no longer stored and are destroyed by the Pre-School Manager.
 - The pre-school has its own camera. Where staff need to use their own equipment to take images these must be transferred onto a disk/memory within 3 days.
 - Photographs and recordings of children are only taken of children if parents provide written permission to do so (found on the individual child's Registration Form).
 - The uploading of photographs onto the website or Facebook of children should only occur after permission has been given by a parent/carer.
 - Any photographs or video clips uploaded should not have a file name of a child, Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing.

4. Web Technologies

4.1 Managing Social Networking and other Web 2.0 technologies

Social networking sites have emerged in recent years as a leading method of communication proving increasingly popular amongst both adults and young people alike. The service typically offers users both a public and private space through which they can engage with other online users, and express themselves creatively through images, web content and their own personal profile page. With responsible use, this technology can assist with the development of key social skills whilst also providing users with access to a range of easily accessible, free facilities. However, as with any technology that opens a gateway to online communication with people, there are a number of risks associated which must be addressed. With this in mind, staff are encouraged to think carefully about the information which they provide on such websites and the way in which it can be manipulated when published (examples of which include Facebook.)

4.2 Social networking advice for staff

Social networking outside of work hours, is the personal choice of all staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Staff should ensure that full privacy settings are in place to prevent anyone other than personal friends from accessing photo albums or personal information.

- Staff are advised against accepting invites from parents until they have checked with them in person that the invite is genuine (avoiding fake profiles set up)
- Staff will ensure that they will not post anything online, or in an email or text, that may damage their personal professional reputation, or the reputation of colleagues or bring the pre-school into disrepute. If there is evidence to suggest that reputations have been damaged, or the pre-school brought into disrepute then disciplinary action may be undertaken against the staff in line with the pre-schools discipline procedure.
- There is documented evidence to suggest that social networking can be a highly effective tool for communicating with parents on a **professional** level. The setting has set up a Facebook account to manage and monitor public communications through designated members of staff.

5. Monitoring

- The Business Manager and Pre-School Manager should be monitoring the use of on-line technologies by staff on a regular basis.
- The Management Trustees will also review the policy annually.

6. Managing allegations and concerns of abuse made against people who work with children.

- Please refer to the Allegation Procedure, Section 12 LSCBN, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.
- Allegations made against a member of staff should be reported to the Chairperson within the setting immediately.

7. Disciplinary Procedure for All Pre-School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Management. The Management Trustees will then refer to the pre-school disciplinary guidelines.

Ratified on 11th February 2020

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.