Lloyd Park Children's Charity

Charity number 1102134

8.0 E-safety and Information Communications Technology (ICT) Policy

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.

Procedures

We have a designated team who are responsible for coordinating actions to ensure online safety. Please contact our Information Sharing Leads via email to lpc@tlpcc.org.uk with any queries regarding online safety.

Online Safety

Digital technology is a crucial part of young people's lives in and out of school and a valuable tool for learning. We take online safety and social media use extremely seriously and encourage children to use the internet responsibly and sensibly both at our settings and at home.

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.

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 or distress.

I.C.T Equipment

- The Operations Lead on the senior leadership team ensures that all computers have up-to-date virus protection installed.

- 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 authorised by a senior manager and are stored securely at all times when not in use.

Internet and social media access for children and young people

- 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 not accessed whilst with/ or by children due to the risk of inappropriate content unless approved by SLT with full risk assessment being completed.
- 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.
- Computers/devices for use by children are always 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 managers ensure staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Email

- Children are not permitted to use email in the setting. Parents 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 share information securely at all times.

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

- Personal mobile phones are not used by our staff on the premises during working hours. They will be stored in lockers or locked drawers. Work issued mobiles will be used on the premises but not in areas with children.

- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- Parents and visitors are requested not to use their mobile phones whilst on the premises. We make an exception if a visitor's company or organisation 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 no children are present.
- These rules also apply to the use of work-issued mobiles and devices, and when visiting or supporting staff in other settings.

Mobile Phone (Children)

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in [lockers or a locked drawer] until the parent collects them at the end of the session.

Cameras and videos

Please see our Photography and Filming Policy for information.

Learning Stories for recording children's progress

- Work devices are used to photograph and record evidence for the children's learning stories.
- If Smart tablets are used, they are password protected and photos and videos are removed after being transferred onto the secure server. These are then transferred onto learning stories format and hard copies are printed. Once the story has been created and printed, photos and videos are deleted.
- If a camera is used, the photos are transferred onto learning stories format and hard copies are printed. Once the story has been created and printed, photos and videos are deleted.

Cyber Bullying

We ensure all incidents of cyber-bullying are logged and managed. All online safety issues and incidents are managed in line with the charity's safeguarding policy. 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

Team Members 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 photographs 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 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
- report any concerns or breaches to the designated team.
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity.
- not access or attempt to access inappropriate material via social media.
- Acceptable use of the Charity's internet only. Staff must not use social media chat rooms or networking sites with children.
- only carry out parent/career communications through the closed Facebook account. Users must adhere to the rules of the group. If staff are friends with parents/carers outside of a professional capacity then this should be shared with their line manager and any conflict of interests discussed and boundaries agreed.

Use/distribution of inappropriate images

- Team Members 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 is behaving

inappropriately, team members are advised to follow our Safeguarding Whistleblowing Procedures.

Policy Name	E-Safety
Version Number	V3 – Replacing Online Safety 2020 Policy
This policy was developed by	Information Sharing Leads.
These people were consulted/ involved in developing the policy	Safeguarding Team Senior Leadership Team Governance Group
This Policy was adopted by	Trustee Board
Date	November 2024
Signed	
Name	Bisi Oyekanmi
Role	Chairperson
Next Review Date	November 2025