Manchester Progressive Education Children's Community

Alexandra Park
Children's Learning Community
a personal learning journey together

Digital Safeguarding Policy

At Alexandra Park Children's Learning Community, we embrace technology and encourage the children, where appropriate, to do so too.

Each room in the setting now has their own tablet, which the staff will use to take photographs (with prior parental consent) and write observations to document their achievements and to inform planning and next steps. We understand that we must record this information in line with data protection laws, and never share photographs of your child without your prior consent.

The images and observations of your child will be uploaded to the secure program "Tapestry", which is used to track your child's development through the Early Years Foundation Stage. Each parent will be given the login details to log in and see their own child's progress. This policy is an extension of the ICT policy that is already in place in the centre but is also more specific in relation to the tablet. Also it is written in line with our Mobile Phone Policy, Social Networking Policy, Children's Anti-Bullying Policy, Confidentiality policy and the government guidance Safeguarding Children and protecting professionals in Early Years Settings: Online Safety Guidance for Practitioners 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

Digital Safeguarding Procedure

- Staff each has access to their room's tablet and computers. They are given individual logins to add information for their key children.
- Staff are only allowed to access our online Journal Tapestry while at work, during working hours and not after 6pm.
- We never share a child photo, video, documents with other parents on Tapestry. We delete all personal details on Tapestry of staff, children and parents when leaving our setting.
- Senior management will do spot checks of when staff are logging in to update details of their key children. Staff found logging in after working hours will be subject to a disciplinary.
- No parent will be given the login details of any other children.
- Each room has their own tablet which is only used for Tapestry and photography. Staff are not permitted to keep children's photograph and videos for themselves without permission of parents o to share them with others.
- Staff are not permitted to use any other applications on the tabletor computers including Social media and Email. If found doing so they will be subject to a disciplinary.
- Children are able to use the tablets for photography or watching appropriate videos chosen by the facilitators/key workers. This can only be done on supervised basis. Any staff

member allowing children to use a tablet without constant supervision will be subject to disciplinary.

- No tablet or computers shall be taken out of the centre under any circumstances, if any member of staff is found to have breached this, then that shall be considered a disciplinary offence.
- All tablets and computers at the close of day must be put away in a secure locked office.
- If you have any suspicions or concerns about another staff member use of the tablet and computers, please report it immediately to a director.
- Please clean tablet screen with special screen wipes.
- All devices in our setting (computers and tables) are filtered and monitored by RM NET support. E-safe for Safeguarding alert on escalating back to Safeguarding Team.
- As standards all devices in APCLC are filter and monitor to ensure the high level of Safeguarding provision.
- All staff , managers and directors will receive digital safeguarding training during the Induction process, General Safeguarding Staff training and online training.
- Parents receive information, advice and guidance (IAG) about Digital Safeguarding /Online Safety by Memos on Tapestry, leaflets and emails on regular basis. All information is to guide and educate our parents to support their children at home.

- Please speak to any director to clarify any points raised in this policy.

The risks that should be recognised include:

- prolonged exposure to online technologies, particularly from an early age
- exposure to illegal, inappropriate or harmful content
- grooming and exploitation
- cyberbullying
- making, taking and distribution of illegal images and “sexting”
- physical, sexual and emotional abuse
- identity theft
- privacy issues
- addiction to gaming or gambling
- pressure from the media and targeted advertising
- theft and fraud from activities such as phishing
- viruses, malware, etc
- damage to professional online reputation through personal online behaviour.

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 by signature or email.

- Inform parents 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.

Date – August 2021 Signed Manager-

Review August 2022 Signed Director -