Glaisdale Playgroup
E-Safety Policy
Use of Mobile Phones, cameras and other devices capable of taking and storing images.

Glaisdale Playgroup is committed to safeguarding the children in our care, this is the responsibility of the delegated staff member – Janet Houlston, supported by deputy – Helen Purtill and the committee.

The use of images, taken on playgroup cameras, tablets and stored on the playgroup laptop, is for observational purposes. These are used in children's photo learning journal and the Tapestry Learning Journal online. These detail a child's development and progress through the areas of learning during their time in the playgroup. They can be displayed on the playgroup website, and in publicity articles with parental permission. (No names used.)
The laptop on which images are processed and stored is used solely by playgroup staff for the purpose of conducting playgroup business. Images of children will be deleted when they have left the setting, images with more than one child will be stored until the youngest child leaves, a maximum 4 ½ years.

Information Communication Technology (ICT) equipment:-

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The NYCC internet access that we use ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

Staff:-

Any device brought into the setting capable of taking images must be placed in the black box on the entry table.
While at playgroup **staff should not** use their mobile phone, if a family member needs to **contac**t a member of staff **for emergencies** this should be **via the playgroup mobile 07854 840516**. Please give this number to your immediate family.
Please **stress that you are at work** and not able to speak to anyone unless it is an emergency.
Staff will not use their personal mobile phone, camera or any other ICT device capable of taking images in the room or outside while children are present.
No member of staff will take or store images of playgroup children on their personal equipment.

Only emergency calls should be taken during sessions, preferably on the playgroup telephone, staff are requested to make use of the playgroup mobile if they need to make a call.

Parents:-

Parents are asked **not to use** their own mobile phones, cameras or other devices during sessions.
During sessions or at events if you would like a photograph please ask a member of staff to take it on the playgroup camera or tablet and the image will be sent electronically to the parent concerned, remember if photos show other children the sharing of these will not always be possible.
If images are taken at events with everyone's permission, they **must not** be displayed on social networking sites or published. Names of children **must not** be used. Some parents do not wish their child's image to be publically displayed, please respect their wishes and maintain confidentiality at all times.

Staff, parents, visitors:-

- If anyone **needs** to bring their phone into the playgroup building we request that **all devices capable of taking images** be placed in the black box, clearly marked. The phone can only removed in an absolute emergency or at time of departure.
- If a call comes in the recipient should answer the device outside the gate firstly notifying a member of staff who can ensure there are no children present. This is to ensure that **no images** are taken of any child in our care. 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 will 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.

Internet Access:-

- Children do not normally have access to the internet and never have unsupervised access.
- If staff access the internet with children it will be for the purposes of promoting their learning,.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.

- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
  - only go on line with a grown up
  - be kind on line
  - 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
- Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.
- If a second hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- 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.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk**.**
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

Due to us using the school internet access, on the staff computer, only certain safe internet sites can be accessed as NYCC blocks any unsafe sites.

Social Media:-

- Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- Staff should not accept service users, children and parents as friends due to it being a breach of expected professional conduct.

- In the event that staff name the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.
- Staff observe confidentiality and refrain from discussing any issues relating to work
- Staff should not share information they would not want children, parents or colleagues to view.
- Staff should report any concerns or breaches to the designated person in their setting.

Parents are reminded that they have agreed, on registration form, **not** to discuss, share images etc. on these sites any breach may result in your child's place at playgroup being reviewed.

Electronic learning journals for recording children's progress:-

- Managers seek permission prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.
-

Storage of Information:-

- Only necessary information is stored on the laptop, we are registered with the ICO, Information Commissioners Office, exemption from payment May 2014, and provide information about Data Protection to parents.
- We only use the information held as specified in our policies and documents following GDPR 2018 rules. The information is used to aid in the running of the group and may need to be shared with the Local Authority and OFSTED as a legal requirement.

Use and/or distribution of inappropriate images:-

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed
- Staff are aware that grooming children and young people on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

This policy was adopted on.....

(Signed on behalf of the committee by) .....