E-Safety

Online Safety

It is important that children and young people attending Pathways 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 Pathways ensures that all computers have up-to-date virus protection installed.
- Tablets are used by practitioners for the purpose of observation, assessment, and planning and to take photographs for individual children's learning journeys
- We also have tablets for children, these are used for education purposes, and an adult will always be with them.
- Tablets remain on the premises and are always stored securely when not in use.

Internet access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early leaning are used (e.g. CBeebies).
- 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 Pathways 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.
- Any computers or tablets used by children are sited in an area clearly visible to staff and are monitored.
- 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 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.
- Role model safe behaviour and privacy awareness.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately.

Personal mobile phones and other internet-enabled devices – staff and visitors

- Personal mobile phones and internet enabled devices are not used by staff at Pathways during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe space.
- Work mobiles are used for phone calls, communication between both rooms and tapestry, you may see staff on these devices for this purpose.
- In an emergency, personal mobiles may be used with permission in a safe place.
- 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 personal mobiles or other internet enabled devices on outings.
- Members of staff do not use personal equipment to take photographs of children.
- Parents/carer 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 phones still should be stored away from any areas that children access and the setting phone number given so that they are still contactable if needed. Visitors are advised of a private space where they can use their mobile.

Cameras and videos

- Members of staff at Pathways do not bring their own cameras or video recorders to the setting.
- Photographs/recording of children are only taken for valid reasons, e.g. record learning and development, or for displays, and are only taken on equipment belonging to the setting. If I child was to become uncomfortable with us doing this, we would not force this.
- Camera and video use is monitored by management.
- 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.
- Parental consent is always gained for photographs used for publicity.

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 Pathways 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 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 can access it
- do not add service users/children/parents as friends. If requested by parents use your personal discretion as to whether you accept. You must always remain professional.

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 Pathways is behaving inappropriately, staff advise the designated safeguarding lead who will follow the relevant procedure.