Safeguarding children, young people and vulnerable adults procedures

CP3 E-Safety (including all electronic devices with internet capacity)

Policy statement

Our setting accesses the Internet in a safe way so that the children may learn to use this tool to help enhance their knowledge and understanding about the world in which they live.

We are committed to ensuring the children's safety at all times and have taken the relevant and required steps to minimise any risk which are detailed in 'Procedures' below.
We will continually monitor and update our knowledge and safety features on the computer to ensure any risks are greatly reduced. We will check we comply with all aspects of safety by completing the attached audit annually.
We will ensure that parents/carers are fully informed about all the safety features we have in place so they may feel confident that their children's safety is of paramount importance.

Procedures

- The pre-school will use the Internet Service Provider (ISP) that the church uses – STRATOTEL.
- The pre-school will use the Internet telephone service that the church uses - this is supported by the ISP named 8 x 8
- The ISP has demonstrated they provide adequate filters and protection so that the risk of unsuitable or inappropriate materials filtering through is minimised.
- However, we appreciate it is our responsibility, as the user, to ensure we have put as many safeguards in place as possible and so we have installed the security protection programme **McAfee** which will be reviewed annually.
- A firewall has been installed in order to help protect the computer from the spread of viruses or worms.
- Little Fishes does have its own email address for business use only. The address is littlefishes@stbbc.org.uk

Online Safety

- 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

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 designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.
- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children's learning journeys.
- Taking photographs of the children is one way in which we support children's development and engage parents in their children's learning. The iPad used within the setting, either on site or on outings, will be the setting's designated iPad.
- Tablets and iPad are stored securely at all times 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 learning are used (e.g. CBeebies).
- No personal purchases will be made from any devices belonging to the setting, ensuring that no personal information is recorded or stored on any device.
- 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.

Procedure for dealing with Undesirable Materials or Websites

If, in the very unlikely event, our safety procedures were breached and unsuitable or inappropriate materials were accessed the following procedures will be followed –

- The member of staff closest to the ICT equipment would put themselves in front of the screen whilst encouraging the child/ren to leave the area. Another member of staff would steer all the children away from the ICT equipment (and out of the room if the images were extremely offensive).
- They would put a covering over the screen until they had completed the entire procedure process. This is to ensure the information we require to report the incident is not lost before a written note can be made of it.
- The member of staff would **write** the name of the website into the computer record book which is kept in the locked filing cabinet in the file for Safeguarding. Other information to be recorded in this book is the date and time of the breach and the name/s of the child/ren involved. (See information on "Committing an Illegal Act – Did You Know?" located in the policies and procedure folder and the computer folder).
- The member of staff would then close down the computer completely.
- The designated person in charge of internet safety – Little Fishes Manager - would inform the Internet Watch Foundation – www.iwf.org.uk. This site is the UK's hotline for reporting illegal content and they have the authority to investigate any complaints and breaches of internet safety. If that officer is absent, the Child Protection Officer or Supervisor for the session would be responsible for reporting the incident.
- In the highly unlikely event of a child being exposed to unwanted images, the child/ren
- would be observed closely for the remainder of the session and the designated practitioner would act sensitively in any discussion that took place. A record of the conversation and the incident would be recorded on a Child Protection record slip which would be signed by the parent/carer when they are told about the incident; this would be kept with the Child Protection documents.

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

- Personal mobile phones and internet enabled devices are not used when staff are working with children. This does not include breaks where personal mobiles may be used off the premises or in a safe place e,g, the children's room by the main telephone. The setting manager completes a risk assessment for where they can be used safely.
- In an emergency, personal mobile phones may be used in a safe place with permission.
- 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 mobile phones on an outing in the community. On this occasion the Manager or Deputy Manager take their personal mobile phone with them in case of an emergency. They do not receive calls during this time, nor do they take photographs of the children.
- Members of staff do not use personal equipment to take photographs of children.

- Parents 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. Visitors are advised of a private space where they can use their mobile.
- Assessors are asked to prove they have immobilised the camera part of their device so that photographs or videos are not taken of the children without our knowledge. They are advised the manager may wish to look at their devices before they leave to ensure no unauthorised photographs or videos have been taken.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.
- Camera and video use is monitored by the setting manager.
- At pre-school events, parents/carers are reminded that if they should take a photograph of their child and it includes another child, they are not to share this photo in any way unless they have that parents/carers permission. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- Parents must not use photos from their child's online tapestry account for social media use.
- Photographs/recordings of children are only made if relevant permissions are in place.
- A designated person – Joanne Waelend – is responsible for printing the photographs from our iPad and collects them promptly from the printer which is situated within the main church office. All church staff are DBS checked and only authorised people are permitted to enter the office. At this point the photographs are used for displays within the setting and Senco visual aids. The other is an electronic copy, stored on the setting's iPad, should we need to refer to it at a later date. Photographs are stored on the iPad for the duration of the child's time with us and then deleted.

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 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 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 are able to access
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or breaches to the designated person in their setting
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed.

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 is behaving inappropriately, staff advise the designated person who follow procedure Allegations against staff, volunteers or agency staff.

Email

- Parents and staff are not 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.

Guidance

https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings

This policy was adopted at a meeting of	Little Fishes Pre-School
Held on	20/9/11
Date to be reviewed	Reviewed: Autumn 2022
Next review:	Autumn Term 2023
Signed on behalf of the management committee	Vicky Baker – Chair
	Tracy Parkins – Manager