

Sacred Heart Pre-school

Heys Street
Thornton-Cleveleys
FY54HL

Tel: 07835711921
EY 318019

**(17) Online safety (inc. mobile phones and cameras) (EYFS – 3.4)**

**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**

The Designated Safeguarding Leads are ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to **Chelsea Porter, Hannah Curtis and Clare Hansford.**

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

***Content:*** *being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;*

***Contact:*** *being subjected to harmful online interaction with other users; for
example commercial advertising as well as adults posing as children or young adults; and*

***Conduct:*** *personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.*

Within preschool, we aim to keep children, staff and parents safe online. Our safety measures include:

* Ensuring we have appropriate antivirus and anti-spyware software on all devices and update them regularly
* Ensuring content blockers and filters are on all our devices, e.g. computers, laptops, tablets and any mobile devices
* Ensuring all devices are password protected and screen locks.
* Monitoring all internet usage across the setting
* Providing secure storage of all nursery devices at the end of each day
* Ensuring no social media or messaging apps are installed on nursery devices
* Reviewing all apps or games downloaded onto devices ensuring they are age and content appropriate
* Using **only** pre-school devices to record/photograph children in the setting.
* Never emailing personal or financial information
* Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
* Teaching children how to stay safe online and report any concerns they have
* Ensuring children are supervised when using internet connected devices
* Providing training for staff in online safety and understanding how to keep children safe online. We encourage staff to complete the E-Safety course on NoodleNow!
* Staff model safe practice when using technology with children and ensuring all staff abide by an acceptable use policy; instructing staff to use the work IT equipment for matters relating to the children and their education and care. No personal use will be tolerated.
* Monitoring children’s screen time to ensure they remain safe online and have access to material that promotes their development. We ensure that their screen time is within an acceptable level and is integrated within their programme of learning
* If any concerns arise relating to online safety, then we will follow our safeguarding policy and report all online safety concerns to the DSL.

**The DSL will make sure that:**

* All staff know how to report a problem and when to escalate a concern, including the process for external referral
* All concerns are logged, assessed and actioned in accordance with the settings safeguarding procedures

**Cyber Security**

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that Cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity e.g. scam emails. All staff are reminded to follow all the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the NCSC Suspicious Email Reporting Service at report@phishing.gov.uk

**Phones and Cameras**

*Mobile phones – 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.

*Mobile phones – staff and visitors*

* Apart from staff lunch breaks (see below), personal mobile phones are not used by our staff on the premises during **working hours**. They will be stored securely in a locker.
* When staff are on their 30 minutes lunch break, there is no staff room for them to go to for their lunch, therefore they go into a designated area in the pre-school room. They are all aware of confidentiality and the safeguarding of the children and are allowed, to access their phones during this time with discretion and with permission from the manager who will monitor them closely.
* 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 when visiting or supporting staff in other settings.

*Smart watches*

* Staff are encouraged to not wear smart watches in pre-school
* Where staff ask to wear them, they are asked to keep them in a do not disturb mode – disconnected from their phone so they do not have access to any non-work related apps or phone features in the working day
* No watches will be worn which contain camera features

*Cameras and videos*

* Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting.
* Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development, or for displays within the setting, with written permission received by parents. Such use is monitored by the manager.
* Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have a right to photograph anyone else’s child or to upload photos of anyone else’s children.
* If photographs of children are used for publicity purposes, parental consent must be given, and safeguarding risks minimised.

*Social media*

* Parents are given information about our Facebook page and website. They are informed that photographs of the children who currently use the setting may be posted, without being named. Parents are given the option of opting out of this.
* 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.
* 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.

*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).

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

**Policy adopted/implemented by SACRED HEART PRE-SCHOOL in:**

August 2023

**Date to be reviewed:**

Yearly

**Signed on behalf of management team:**

Chelsea Porter (Deputy) – 24/8/23

**Reviewed by**:

Chelsea Porter (Manager) – September 2024