Online & Social Networking Policy

At Tender Care Nursery we aim to ensure the safety of all the children in our care.

"OUR SETTING IS COMMITTED TO SAFEGUARDING AND PROMOTING THE WELFARE OF CHILDREN, YOUNG PEOPLE AND ADULTS AT ALL TIMES AND EXPECTS EVERYBODY WORKING WITHIN THIS SETTING TO SHARE THIS COMMITMENT."

Our nursery is aware of the growth of internet and the advantages this can bring. However, it is also aware of the dangers it can pose and we strive to support children, staff and families to use the internet safely. We refer to *'Safeguarding children and protecting professionals in early years settings: online safety considerations'* to support this policy.

The Designated Safeguarding Leads are ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to the DSL;

SETTING	DESIGNATED LEAD	DEPUTY LEAD
Canterbury Tender Care	Liz Francis	Saleha Islam

Online Safety

The nursery will audit IT use to establish if the online policies are adequate, appropriate and effective when all nursery policies are reviewed yearly. All staff will be given the following information and its importance will be explained.

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 categorized 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.*

Computer and Internet Use

In common with all nurseries Tender Care Nursery uses computer, photographic and video technology to enhance the educational experiences of the children in our care.

- During these activities' children do not have access to the internet, they have full access to the children's computer and laptops with staff supervision.
- On a regular basis we take pictures of children involved in nursery activities, which we use for teaching, observation and publicity purposes with extra consent
- The Main nursery computer is connected to the internet, the pre-school computer and laptops do not have internet access at Westbury Tender Care. The tablets staff use for observations at Zakia and Canterbury are password protected, children do not have access to these. Any time they are used with children this is supervised. All tablets and the ICT room Genie have child protections and no social media or adult applications installed.
- We will endeavour to ensure that the use of internet derived materials by staff complies with copyright law.

Social networking

It is likely that many staff/ parents belong to a social networking site (eg. Facebook, Twitter, My space). Nursery policy states that:

- Access to social network sites is not permitted at nursery.

Nursery:

- With regards to nursery social media we do not allow others to post on our social media pages, i.e. designated person/ management can post on the page
- Have separate permission to use any images for any open public pages that we use for marketing purposes
- We monitor comments on all posts and address any concerns immediately.

Staff:

- Staff do not name the nursery they work for
- Staff remain professional and do not discuss nursery business
- Staff do not name or discuss any information regarding other staff members, children or parents associated with the setting past or present
- Staff do not request or accept the invitation to befriend nursery parents/carers at any time
- Staff must ensure that privacy settings are set to private and that content is appropriate, including photos and language used
- Staff are not to send private messages to any parent's/family members
- Staff will not direct any parent questions relating to work via social networking sites, to the manager
- Ensure any posts reflect their professional role in the community (e.g. no inappropriate social event photos or inappropriate comments i.e. foul language)
- Report any concerning comments or questions from parents to the manager/safeguarding lead
- Follow the staff behaviour policy
- Not post anything that could be construed to have any impact on the nursery's reputation or relate to the nursery or any children attending the nursery in any way
- Will follow this in conjunction with the whistle blowing policy.

-

Parents:

- Parents are strongly requested not to invite staff members to be friends via a social network
- Parents are strongly requested not to discuss nursery business on any network site. All issues or concerns must be discussed with the nursery staff or committee.
- Parents are strongly requested not to place photos from a nursery event of any kind onto a social network site

Child Images

As a nursery we regularly take individual or group photographs of the children in our care. These images may be used for display inside the nursery areas, in our prospectus or on our website. We also use the images for teaching, observation and publicity purposes. The nursery has been using photographs of children in such ways for many years with no problems. However, to comply with the Data Protection Act 1998 the nursery requires permission from parents/carers to take these photographs. As a nursery we promise to:

- Seek parental permission for images to be taken or used for teaching, observation and publicity purposes for every child in our care
- Not identify individual children in our displays, prospectus or on our website without prior parental consent
- Use only the nursery cameras to take photographs
- Ensure all staff are aware that the use of personal mobile phones to take photos or videos is not permitted – failure to adhere to this will lead to disciplinary action
- Ensure that visitors are aware that the use of mobile phones to take images or record videos is not permitted
- Strongly request that parents do not place photos taken at a nursery event of any kind onto a social network site
- Never use images taken at nursery or a nursery event and place onto a social network
- Events such as, Sports day, Outings, Christmas and Fundraising Events may be recorded by video and photographs by staff but always in full view of all attending. Parent and carers are not allowed to film or take pictures.
- On occasion we might like to use photographs of the children taking part in an activity to advertise/promote our pre-school via our Web site etc; however, in this instance specific parental permission for these events would be required.

Within the nursery 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. Practitioners are re-minded to use complex strong passwords and they are kept safe and secure, changed regularly and are not written down

- Monitoring all internet usage across the settings
- 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 nursery 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
- Using tracking software to monitor suitability of internet usage (for older children)
- Not permitting staff or visitors to access to the nursery Wi-Fi
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not; comparing people in real life situations to online 'friends'
- 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 (see acceptable IT use policy)
- 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
- Making sure physical safety of users is considered including the posture of staff and children when using devices
- Being aware of the need to manage our digital reputation, including the appropriate-ness of information and content that we post online, both professionally and personally. This is continually monitored by the setting's management
- Ensuring all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses and telephone numbers. This is to protect staff, children and parents
- Signposting parents to appropriate sources of support regarding online safety at home including digital parenting magazine and NSPCC website.

If any concerns arise relating to online safety, then we will follow our safeguarding policy and report all online safety concerns to the DSL.

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

Legal Framework

The Data Protection Act 2018

This policy was adopted on	Signed on behalf of the nursery	Date for review
06/01/2026	Liz Francis – Head of Operations	06/01/2027