45. Use of Technology and Internet Policy

Legislation

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679).

Related policies

- Whistleblowing
- Safeguarding Children and Child Protection
- Data Protection and Confidentiality

This policy describes the rights and responsibilities of staff, students and other adults in the setting using resources such as computers, tablets, the internet, landline and mobile telephones, and other electronic equipment. It explains the procedures everyone is expected to follow and makes clear what is considered acceptable behaviour when using them. These devices are a vital part of our business and should be used in accordance with our policies in order to protect children, staff and families and in the best interests of the business.

Our nursery is aware of the growth of the internet and technology and the advantages this can bring to everyday life. 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 Lead (DSL) is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to Carol Daly (Manager and DSL) or in her absence a Deputy DSL Jodie Hursthouse (Assistant Manager), Chelsea Dakin, Ahmreen Naz and Seren Brown (Room Leaders).

The Professionals' Online Safety Helpline (0344 381 4772 / helpline@saferinternet.org.uk) can be accessed for advice and support by any staff member.

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation, radicalisation and sexual predation with technology often providing the platform that facilitates harm.

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

1. ***Content:*** *being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views*
2. ***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*
3. ***Conduct:*** *personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.*

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 have screen locks. Practitioners are reminded to use complex strong passwords, keep them safe and secure, change them regularly and not to write them down
- 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, other than those used by the managers for this purpose
- Reviewing all apps or games downloaded onto devices ensuring they are age and content appropriate
- Using only nursery devices to record and /or photograph children in the setting
- Ensuring that staff do not to use personal electronic devices with imaging and sharing capabilities, including mobile phones, smart watches and cameras
- Never emailing personal or financial information unless through Egress
- 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
- Not permitting staff or visitors private 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'

- When using online video chat, such as Zoom, Teams, Skype, FaceTime etc. (where applicable) discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff, at least annually, in online safety and understanding how to keep children safe online. We encourage staff and families to complete a free online safety briefing, which can be found at https://moodle.ndna.org.uk/
- Staff modelling safe practice when using technology with children and ensuring all staff abide by this policy such as instructing staff to use the nursery IT equipment for matters relating to the children and their education and care only. 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
- Making sure the 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 appropriateness of information and content that is posted online, both professionally and personally. This is continually monitored by the setting's management
- Staff must not friend or communicate with parents on personal devices or social media accounts (see below)
- Ensuring all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. Tapestry, 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

If any concerns arise relating to online safety, then we will follow our Safeguarding Children and Child Protection 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 nursery's safeguarding procedures

- Parents are supported to develop their knowledge of online safety issues concerning their children via newsletters and the notice boards
- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern
- Staff have access to information and guidance for supporting online safety, both personally and professionally
- Under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material.

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.

Security and passwords

All electronic devices will be password protected, and passwords will be updated on a regular basis. Passwords for our systems are confidential and must be kept as such. You must not share any passwords with any other person; in particular you must not allow any other staff member to know or use your password.

Email

We expect all staff to use their common sense and good business practice when using email. As email is not a totally secure system of communication and can be intercepted by third parties, external email should not normally be used in relation to confidential transactions. In these instances, Egress should be used for external recipients, or documents uploaded to SharePoint or Hubdoc for access by the owners/managers.

Emails must not be used to send abusive, offensive, sexist, racist, disability-biased, sexual orientation based or defamatory material, including jokes, pictures or comments which are potentially offensive. Such use may constitute harassment and/or discrimination and may lead to disciplinary action up to and including summary dismissal. If you receive unwanted messages of this nature, you should bring this to the attention of the manager immediately.

Internet access

You must not use the internet facilities to visit, bookmark, download material from or upload material to inappropriate, obscene, pornographic or otherwise offensive websites. Such use constitutes misconduct and will lead to disciplinary action up to and including summary dismissal.

Each employee has a responsibility to report any misuse of the internet or email. By not reporting such knowledge, the employee will be considered to be collaborating in the misuse. Each employee can be assured of confidentiality when reporting misuse and can do so using the whistleblowing procedure.

Personal use of the internet, email and telephones

Any use of our electronic communication systems (including email, internet and telephones) for purposes other than the duties of your employment is not permitted.

Emergency personal calls need to be authorised by the manager and, where possible, be made on your own personal mobile phone outside the nursery.
Disciplinary action will be taken where:

- The privilege of using our equipment is abused, or
- Unauthorised time is spent on personal communications during working hours.

Data protection

When using any of our systems employees must adhere to the requirements of the General Data Protection Regulation 2018 (GDPR). For more information see our Data Protection and Confidentiality policy.

Downloading or installing software
Employees may not install any software that has not been cleared for use by the manager onto our computers, tablets or systems. Such action may lead to disciplinary action up to and including summary dismissal.

Using removable devices
Before using any removable storage, media which has been used on hardware not owned by us (e.g. USB pen drive, CDROM etc.) the contents of the storage device must be virus checked. Any removable storage media containing confidential and/or personal information must be password protected if it leaves the setting.

Using tablets
All staff must sign the Tapestry user agreement prior to using the tablets for any reason. Tablets are password protected, and the passwords should not be shared beyond the staff working in each room. Tablets may be taken off premises once a signing out sheet has been completed and signed by a manager.

We use tablets in the rooms to take photos of the children and record these directly on to their electronic learning journeys. We ensure that these devices are used for this purpose only and do not install applications such as social media or messaging sites on to these devices.

We carry out routine checks to ensure that emails and text messages (where applicable) have not been sent from these devices and remind staff of the Whistleblowing policy if they observe staff breaching these safeguarding procedures.

Tablets are not for use by the children, and staff are responsible for ensuring that children do not view inappropriate material on the tablets. For example, staff must use a child appropriate search engine (e.g. KidRex, KidzSearch) if children are viewing the tablet when searches are made. Children must never watch any online content (e.g. YouTube videos) that has not been previously watched and checked by a staff member for appropriateness.

Using mobile phones, cameras, smart glasses and other electronic devices with imaging and sharing capabilities

To ensure the safety and well-being of children we do not allow staff, students or other adults in the setting to use personal mobile phones or other personal devices with imaging and sharing capabilities during working hours as this distracts them from their duty of care towards the children and has the potential to place children at risk of harm.

We use mobile phones supplied by the nursery only to provide a means of contact in certain circumstances, such as outings and the school run.

Staff must adhere to the following:

- Mobile phones, or other personal devices with imaging and sharing capabilities are not accessed during working hours. They can only be used on a designated break and then this must be away from the children (e.g. in the kitchen, staff room, office or off site)
- Mobile phones, or other personal devices with imaging and sharing capabilities must be stored safely in staff lockers, Baby Unit kitchen or the nursery office at all times during working hours and must be kept on silent.
- Smart glasses are not to be worn or used on the nursery premises.
- Staff wearing smart watches/Fitbit etc must ensure that these are not connected to the internet during working hours. They can be worn as a time piece, pedometer etc but must not be receiving texts, calls, emails etc.
- No personal device is allowed to be connected to the nursery Wi-Fi at any time without prior authorisation of the manager
- The use of nursery devices, such as tablets and mobile phones, must only be used for nursery purposes
- The nursery devices will not have any social media or messaging apps on them, except those used by management for nursery purposes only
- Any apps downloaded onto nursery devices must be done only by management. This will ensure only age and content appropriate apps are accessible to staff, or children using them
- During outings, staff must only use mobile phones belonging to the nursery
- Only nursery owned devices will be used to take photographs or film videos

- Nursery devices will not be taken home with staff without authorisation and will remain secure at the setting when not in use. If a device is taken home for work/training needs, then the staff member must ensure that it is securely stored (including not being left unattended in a car) and not accessed by another individual. It should be returned to the setting as soon as practically possible.

Parent/Visitor use of mobile phones and smartwatches

Parents are kindly asked to refrain from using their mobile telephones, or other personal devices with imaging and sharing capabilities, whilst in the nursery or when collecting or dropping off their children. We will ask any parents using their phone/device inside the nursery premises to finish the call or take the call outside. We do this to ensure all children are safeguarded and the time for dropping off and picking up is a quality handover opportunity where we can share details about your child. Handovers will not take place if a parent is using a device.

Parents are requested not to allow their child to wear or bring in devices with imaging and sharing capabilities, including Vtech and smart watches. This ensures all children are safeguarded and also protects their property as it may get damaged or misplaced at the nursery.

Parents or visitors remaining on the premises are asked to leave their devices in the nursery office. They are not permitted to use any personal devices with imaging and sharing capabilities on the nursery premises without the prior consent of the manager.

Photographs and videos

We recognise that photographs and video recordings play a part in the life of the nursery. We ensure that any photographs or recordings taken of children in our nursery are only done with prior written permission from each child's parent and only share photos with parents in a secure manner (eg via Tapestry). We will obtain this permission when each child is registered and parents have the right to remove permission at any time by writing to the manager.

We ask for individual permissions for photographs and video recordings for a range of purposes including use in the child's learning journey, for display purposes, for promotion materials including our nursery website, brochure and the local press and for security in relation to CCTV and the different social media platforms we use. We ensure that parents understand that where their child is

also on another child's photograph, but not as the primary person, that may be used in another child's learning journey. Photographs and videos will not be taken in areas where intimate care routines are carried out.

If a parent is not satisfied about one or more of these uses, we will respect their wishes and find alternative ways of recording their child's play or learning.

Staff are not permitted to take any photographs or recordings of a child on their own personal devices with imaging and sharing capabilities, e.g. cameras, mobiles, tablets or smartwatches and may only use those provided by the nursery. The nursery managers will monitor all photographs and recordings to ensure that the parents' wishes are met, and children are safeguarded.

During special events, e.g. Christmas or leaving parties, staff may produce group photographs to distribute to parents on request. In this case we will gain individual permission for each child before the event. This will ensure all photographs taken are in line with parental choice. We ask that photos of events such as Christmas parties are not posted on any social media websites or other platforms areas without permission from the parents of all the children included in the picture.

Social networking

Social media is a large part of the world we live in and as such we need to make sure we protect our children by having procedures in place to ensure safe use.

We use Facebook, Email groups and Tapestry to share posts, pictures and videos of the experiences and activities the children have accessed at nursery, as well as to post updates, reminders and links to best practice.

In order to safeguard children, we ensure:

- We have prior written permission in place from parents before posting any images of children
- Only a member of the leadership team/owners can post on our social media pages
- We 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/student use of social media

We require our staff and students to be responsible and professional in their use of social networking sites in relation to any connection to the nursery, nursery staff, parents or children.

- When using social networking sites such as Facebook, Instagram, or X we ask staff:
    - Not to name the setting they work at
    - Not to make comments relating to their work or post pictures in work uniform
    - Not to send private messages or friend requests to any parents or family members
    - To direct any parent questions relating to work via social networking sites, to the manager
    - To ensure any posts reflect their professional role in the community (e.g. no inappropriate social event photos or inappropriate comments i.e. foul language)
    - To report any concerning comments or questions from parents to the manager or designated safeguarding lead
    - To follow the Staff Development policy in regard to their behaviour online
    - Not to 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
    - To follow this in conjunction with the Whistleblowing policy.

- If any of the above points are not followed then the member of staff involved will face disciplinary action, which could result in dismissal.

All electronic communications between staff and parents should be professional and take place via the official nursery communication channels, e.g. work emails and phone numbers. This is to protect staff, children and parents. If staff are already linked on social media with parents when they join the setting, then they should ensure that all communication remains appropriate. We ask staff not to become linked to parents whilst their child(ren) attend the setting but may do so once they have left.

Parents' and visitors' use of social networking

We promote the safety and welfare of all staff and children and therefore ask parents and visitors not to post, publicly or privately, information about any child on social media sites such as Facebook, Instagram and Twitter. We ask all

parents and visitors to follow this policy to ensure that information about children, images and information do not fall into the wrong hands.

We ask parents **not to:**

- Send friend requests to any member of nursery staff
- Screen shot or share any posts or pictures from the nursery on social media platforms (these may contain other children in the pictures)
- Post any photographs to social media that have been supplied by the nursery with other children in them (e.g. Christmas concert photographs or photographs from an activity at nursery).

We ask parents to:

- Share any concerns regarding inappropriate use of social media through the official procedures (please refer to the Parents and Carers as Partners policy and/or Complaints and Compliments policy)
- Remove any posts related to the nursery if requested, for example due to the post containing other children or having been taken inappropriately in the setting.

This policy was adopted on	Signed on behalf of the nursery	Date for review
30/5/25	C. A. Daly	30/04/2026