06 Safeguarding children, young people and vulnerable adults procedures

# 06.9 E-safety and Learning Journals (including all electronic devices with internet capacity)

**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

**I.C.T Equipment**

* The setting manager ensures that all computers have up-to-date virus protection installed.
* Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children’s learning journeys.
* Tablets remain on the premises and are stored securely at all times when not in use.
* Staff follow the additional guidance provided with the system

**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).
* 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 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.
* All computers for use by children are sited in an area clearly visible to staff.
* 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](http://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.

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

* Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks. The setting manager completes a risk assessment for where they can be used safely.
* Personal mobile phones are stored in office phone compartments.
* In an emergency, personal mobile phones may be used in the privacy of the office 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.
* 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.

**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.
* Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents 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.
* If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

**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](http://www.nspcc.org.uk) or ChildLine Tel: 0800 1111 [www.childline.org.uk](http://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 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 06.2 Allegations against staff, volunteers or agency staff.

**Children’s Learning Journals Policy**

**Policy Statement**

At Coombe Day Nursery we ensure that all children attending our setting have a personal learning journal which records photos, observations and comments, in line with the Early Years Foundation Stage (EYFS), to build up a record of each child’s achievements during their time with us. It also shows each child’s developmental progress through the different age bands of the EYFS.

We are using an online system called Tapestry and this policy sets out how this online system will operate.

**Procedures**

* Once a child starts at our setting they are allocated a Key Person who is primarily responsible for the compilation of their online learning journal, however all staff may add information to it.
* Parents will be given a secure login for the system, which only allows them to access information about their child, so that they can look at the journal and add to or comment on it at any time. We encourage parents to be actively involved in their child’s journal and welcome interaction from parents online.
* Staff will generally update a child’s learning journal whilst working in the setting and time is allocated for staff to do so, however there may be times when it is necessary for staff members to work on them at home.
* Observations may be validated by a Manager or deputy before they are added to the learning journal although this may not always be the case.
* Tapestry should only be used to record a child’s progress and should not replace general communication between either the setting or the Key Person and parents.
* Parental access to your child’s learning journal will be closed on the date your child leaves the setting and parents will be able to download a PDF version of the learning journal to keep.
* The child’s data will be removed from Tapestry.

**Safeguarding and Security**

* The Manager controls all staff and parent access to the online system.
* All staff are subject to Updated Enhanced DBS checks
* All staff are required to sign to agree to abide by this Policy as well as the Staff Behaviour Policy, our Safeguarding Policy and all other policies relevant to their roles.
* At all times staff must ensure that they log out of the system when they are not using it ensuring that nobody else can view information on it. Staff are also not permitted to share their passwords with other staff members or anyone else.
* Staff access to the online system will be immediately revoked if they leave the setting and their details deleted from the system.
* Photos of children will only be taken on the settings tablets which are kept locked up at the setting when not in use and are also password protected.
* Parents will only be given access to their own child’s online learning journal and it is important that parents do not share their passwords with anyone else.
* Our setting complies with all relevant data protection legislation, covering both electronic and hard copy data.
* Tapestry is a secure system and full details of their privacy policy is available by accessing www.tapestry/info

**CCTV Policy**

Coombe Day Nursery is securely monitored by a CCTV surveillance system. The Nursery Manager/Owner is responsible for the operation of the system for ensuring compliance with this policy. The Nursery complies with the Information Commissioners CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

The use of CCTV and the associated images is covered by the Data Protection Act 2018 and GDPR. This policy outlines the nursery’s use of CCTV and how it complies with the Act and is associated with the Nurserys Data Protection policy, the provisions of which should always be adhered to.

Cameras are located at strategic points on the premises. No camera is hidden from view and all will be prevented from focusing on areas of private accommodation such as toilets and nappy changing areas. The digital recorder and single effectiveness of the limited system it is not possible to guarantee that the system will detect every incident taking place on the site.

The system has been installed by the nursery with the primary purpose of monitoring entry and exit through the nursery, to safeguard children and safeguard parents and staff on site.

The system is private and viewing of the recorded images of CCTV will be restricted to the Nursery Manager within the office, also to those staff who need to have access in accordance with the purpose of the system. This is not a “webcam” facility; parents will not have access to view recordings and to safeguard all, will not be shared under any circumstances with any parents, staff, or any other peoples. CCTV footage may only be shared with the Police or Local Authority.