

06.0906 Safeguarding children, young people and vulnerable adults procedures

06.09 E-safety (including all electronic devices with imaging and sharing capabilities)

(Please also see 07.08 Off-site handling & removal of personal/sensitive data from premises, home working and personal device usage procedure)

Online Safety

Our vision is that all children and young people, all parents/carers and all those working with children and young people recognise the risks, dangers and potential harm that may arise from the use of internet, digital and mobile technologies and that they understand how to mitigate these risks and potential dangers and are able to recognise, challenge and respond appropriately to any e-safety concerns so that children and young people are kept safe. (Essex Safeguarding Children's Board Vision).

Children and young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences. Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should outweigh the disadvantages.

(Essex Safeguarding Children's Board E-Safety policy)

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

- Only ICT equipment belonging to the pre-school is used by the children.
- The designated safeguarding lead (manager), on-site administrator/trustee and designated safeguarding lead backup are responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers with access to the internet have virus protection installed.
- There is a Little Doves Christian Pre-School laptop which is used solely by the manager and on-site administrator. The laptop and data storage devices comply with General Data Protection Regulations 2018, Essex County Council 'Information Policy Requirements for Contractors v6 2023'. The pre-school manager ensures that the laptop has up-to-date virus protection installed.

- The designated safeguarding lead (manager), on-site administrator/trustee and designated safeguarding lead backup ensure that safety settings on the computer used by the children are set to ensure that inappropriate material cannot be accessed.

Internet access

- Children do not have access to the internet.
- Any computers and Kindles for use by children are sited in an area clearly visible to staff.
- Children are not permitted to use email in the pre-school. Parents/carers and staff are not normally permitted to use pre-school equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- The pre-school 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, Twinkl).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content unless previously checked and recommended by professionals to extend the children's learning.
- 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.
- 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.

The pre-school manager/deputy/senior room leader ensure staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.

- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: <https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety>)

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

- Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobile phones may be used away from the premises or in a safe place e.g, kitchen/office/outside. The pre-school manager/deputy completes a risk assessment for where they can be used safely.
- If a member of staff/volunteer needs to use their phone in an emergency during a session, they are instructed to find an appropriate time to leave the room, informing another member of staff that they are leaving, and go to an area where there are no children. If a staff member needs to keep their phone on them during a session to receive an emergency phone call e.g. GP call, they must inform the manager/deputy/senior room leader at the beginning of the session (and if necessary, complete the 06.09a Staff permission to keep mobile phone on person during session form). This form states the reason and is also signed by the manager/deputy/senior room leader. To take the call, the staff member goes to a safe area i.e. office, kitchen or outside and returns the phone to the safe place in the kitchen when the call is finished.
- Personal mobile phones are stored in the kitchen except for the manager/deputy/designated safeguarding lead/deputy/backup who need phone access to parents/carers for contact and emergencies.
- Staff ensure that contact details of the pre-school are known to family and people who may need to contact them in an emergency.
- If members of staff and volunteers take their own mobile phones on outings for use in the case of an emergency, they must not make or receive personal call as this will distract them, except if they are on their break.
- Members of staff do not use personal equipment, for example, mobile phones, smart watches/Fit Bits, to take photographs of children on the premises of Navestock Village Hall or on a Little Doves Christian Pre-school outing. The manager may use her own mobile phone to take specific photos of children to add to LD Facebook and website and these are deleted from her phone when no longer needed. Staff who wear smart watches are identified on 08.18 Staff code of practice reminders and smart watch declaration and sign to say that their device does not have a camera.
- Staff and volunteers are PROHIBITED from taking a mobile phone or other electronic device into the toilet area where children are present. As stated above, staff sign on the 08.18 Staff code of practice reminders and smart watch declaration to say that their smart watch does not contain a camera.
- Parents/carers 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, away from the children, where they can use

their mobile device. Similarly, if any parent/carer needs access to their phone whilst in the hall, e.g. to pay a Little Doves bill, they are escorted to a safe place and are supervised whilst the use of the phone is taking place.

- The pre-school parents/carers have access to the pre-school by calling the pre-school mobile telephone (07756 029105) or the manager's personal mobile number, if the manager has given permission for it to be used. The Little Doves phone is kept with the manager/deputy/senior room leader and is used during the session by the manager and staff to contact the parents/carers or other staff if necessary. Designated staff may answer the telephone during a session to deal with any queries and to take messages.
- Children do not bring mobile phones or other ICT devices with them to the pre-school. If a child is found to have a mobile phone or ICT device with them, this is removed and kept on the shelf until the parent/carer collects them at the end of the session.
- If access to a mobile phone is required in the pre-school room, for example, to play music for the children or to look up specific information on the internet for a child's activity, permission is sought from the manager or deputy before the phone is used. Any use of mobile phone in pre-school room is done in full sight of other staff members including manager/deputy or senior room leaders.
- In exceptional circumstances, for example, severely unstable diabetes, a child may need their own personal electronic devices in the room to provide instant feedback information to warn of life-threatening deterioration and to trigger immediate medication release. In such circumstances, healthcare professionals are involved and risk assessments are carried out and recorded.

Cameras and videos

- Little Doves has 3 cameras that are used to take photos of children. There are 5 SD cards that are used to store the photos until they are loaded onto the laptop and stored securely. This is done regularly. Photos are deleted in line with 07.12 Data retention document.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development or for displays, Facebook or the website. Photos are only taken on equipment belonging to the pre-school unless in specific circumstances when permission is given by the pre-school manager or deputy (see below). Any photos to be added to the website/newsletter are transferred to the off-site administrator via secure media and are held in line with 07 Record keeping policy and procedures and 07.12 Data retention document.
- Permission is sought from the parent/carer on the 09.01b Registration Sessions Requested and Permission Form which parents/carers complete before the child starts at the pre-school. Photographs/recordings of children are only made if relevant permissions are in place.
- Members of staff do not bring their own cameras or video recorders to the pre-school, however, in certain circumstances a designated member of staff may be authorised by the manager/deputy to use their own camera to:

- take photographs e.g. Christmas or summer leavers photos. In this case a Little Doves SD card will be used, the photos deleted, and the card returned to Little Doves when no longer required
- to record stories and rhymes to upload onto Little Doves Friends Closed Facebook page
- to record short videos to share on Little Doves Friends Closed Facebook page.

Any photos and videos taken are done so in full sight of other members of staff including manager/deputy or senior room leaders.

- Camera and video use is monitored by the pre-school manager/deputy.
- Where parents/carers request permission to photograph or record their own children at special events, general permission is first gained from all parents/carers for their children to be included in the 09.01b Registration Sessions Requested and Permission Form. Parents/carers are told they do not have a right to photograph or upload photos of anyone else's children. If permission is not given by a parent/carer, the manager/deputy/senior room leader makes all efforts to keep the child out of other parents/carers' photos. At an event, the manager/deputy reminds parents/carers to only take photos of their own children.
- If photographs are used for publicity, parental/carer consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their pre-school on it.
- Some visiting health care professionals, for example, physiotherapists, occupational therapists, educational psychologists use their own internet enabled device to take photos/videos of the child in their care to assess the child's progress. The visiting healthcare professional will have sought permission to do this from the parents/carers prior to the visit.
- Any visitor with a webcam on their laptop computer or other electronic imaging device is asked to turn it off/immobilise it or cover it. If a visitor's company or organization operates a lone working policy that requires contact with their office periodically throughout the day, the visitor will be advised of where they can go to use their laptop computer where there are no children present.
- These rules also apply to the use of work-issued mobile phones and when visiting or supporting staff in other pre-schools.
- All visitors, volunteers and students are informed of this policy.
- In the event of an allegation being made against a member of staff, an investigation will be conducted by the manager/deputy/management team and if found necessary the existing grievance procedure will be followed.
- The photographs are printed at Little Doves using its own printer except the Christmas or summer leavers photos which may be taken to a reputable photo processing shop to develop.
- The photographs on the laptop, Facebook and website are retained in line with 07.12 Data retention document.

- Any new technology devices will be reviewed by the management team and all relevant procedures will be adapted accordingly.

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/carers and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 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 pre-school. Any communications or content staff publish that causes damage to the pre-school or any of its employees, children or families may amount to misconduct or gross misconduct and could lead to dismissal. There will be no mention of the pre-school, names of staff, committee members or attending children or their families. This includes indirect reference to people or incidents surrounding them. These can easily be worked out or misinterpreted with disastrous results. Staff members should observe confidentiality and respect the privacy and the feelings of others.
- be aware that comments or photographs online may be accessible to anyone and should use their judgement before posting.
- be aware that images, such as those on Snapchat/Instagram 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/carers 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/carers as friends, as it is a breach of professional conduct and not engage in personal communication, including on social networking sites, with children and parents/carers with whom they act in a professional capacity. However, because Little Doves is a local community pre-school, staff and parents/carers are often friends outside of the pre-school and before a child starts at the pre-school. In these circumstances, the staff are asked to make the manager/deputy aware of any friendships, a risk assessment is undertaken and an agreement in relation to boundaries is agreed.
- report any concerns or breaches to the designated person/deputy/backup designated person in their pre-school.

- Employees (except manager or staff member authorised by manager) must not log onto or communicate via any social networking site during working hours. Online times and times of posts can be seen by other users and may assume that the pre-school allows access within the pre-school compromising the safety of the children in the pre-school. Staff are allowed to log on or communicate on a social networking site during their designated break keeping in line with all the above guidelines.
- Employees of Little Doves Christian Pre-school should NOT identify themselves as working with children – this can lead to being a specific target of unscrupulous members of the web in order to gain access to children for paedophile reasons.

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/deputy/backup designated person who follow procedure 06.2 Low level concerns and allegations of serious harm or abuse against staff, volunteers or agency staff.

01/12/2024 V6