



# Crestwood Pre-school

## Safeguarding and Welfare Requirement: Child Protection

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff and cover the use of electronic devices and cameras in the setting

### Child Protection

#### 1.6 Use of electronic devices including cameras (including social media)

##### 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

- Our designated person responsible for co-ordinating action taken to protect children is:  
Clare Evans

##### Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used with the children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All devices are password protected so can only be accessed by staff.
- All staff ensure their tablets or laptops remain secure when they are taken off the premises. They do not share them with another person, and they remain accountable for any loss or damage caused by removing them off the premises. Staff ensure that our safeguarding policy is adhered to at all times when using their electronic device either on or off site.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.
- ICT equipment is not to be taken into the toilet area by any individual. If an observation is required around handwashing 2 members of staff need to witness this.
- If staff want to wear a Smart watch, they will allow the manager to check it first to ensure it cannot take independent photos. If it can perform this function, it will be disconnected to ensure that photos cannot be taken. All staff will allow the manager to do spot checks at any time. Any member of staff found to be in breach of this will face disciplinary procedures.
- Volunteers and work experience students must disconnect their smart watch from their mobile phone when at the pre-school.

##### Internet access

- Children never have unsupervised access to the internet.

- If staff access the internet with children for the purposes of promoting their learning, written permission on their enrolment form is gained from parents who are shown this policy.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are taught the following stay safe principles in an age-appropriate way prior to using the internet.
  - only go online with a grown up
  - be kind online
  - keep information about me safe
  - only press buttons on the internet to things I understand
  - tell a grown up if something makes me unhappy on the internet
- Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- If a second-hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- Staff report any suspicious or offensive material, including material which may incite racism, Bullying, discrimination or radicalisation to the Internet Watch Foundation at [www.iwf.org.uk](http://www.iwf.org.uk).
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at [www.ceop.police.uk](http://www.ceop.police.uk).
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with the parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or [www.nspcc.org.uk](http://www.nspcc.org.uk), or Childline on 0800 1111 or [www.childline.org.uk](http://www.childline.org.uk).

#### Email

- Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children by themselves.
- Staff send and share information securely at all times.

#### 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 the office cupboard until the parent collects them at the end of the session.

#### Mobile phones - staff and visitors

- Personal mobile phones are not used by our staff on the premises during their working hours. They will be stored in the office.
- 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, students 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. Parents may use their phone to obtain contact information when completing forms in the presence of a member of a member of staff.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.

#### Cameras and videos

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting, unless permission is given by the manager. Risk assessments will be in place to ensure this is of low risk to the children.
- 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 (see the Registration form). 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, for example, ensuring children cannot be identified by name or through being photographed in a sweatshirt with the name of their setting on it.

#### Social media

- 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.
- Staff should not accept service users, children and parents as friends due to it being a breach of expected professional conduct. The only exception to this is if a staff member is already a friend to a parent before they join the setting. If this is the case, then staff will adhere to all policies to ensure total professionalism and any breach of this will result in disciplinary action being taken.
- If any member of staff is contacted on their personal Facebook messenger, they will ensure the parent has the correct method of contacting the Pre-school or the manager.
- 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.
- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly

prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

#### Electronic learning journals for recording children's progress

- All children's files are computerised and every parent signs to agree to this. Only the child's Parent(s)/Guardian(s) who sign up with a secure password and Pre-school staff can access the children's files.
- Staff adhere to the guidance provided with the system at all times.

#### Use and/or distribution of inappropriate images

- Staff are aware that it is an offence to make, possess and 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 online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

#### Further guidance

- NSPCC and CEOP Keeping Children Safe Online training: [www.nspcc.org.uk/what-you-can-do/getexpert-training/keeping-children-safe-online-course/](http://www.nspcc.org.uk/what-you-can-do/getexpert-training/keeping-children-safe-online-course/)

#### Legal framework

##### Primary legislation

Children Act (1989) (2004) (2006)

Protection of Children Act (1999) (2003) (2004)

Data Protection Act (1998) (2003)

The Children Act (Every Child Matters) (2004) (2006)

Safeguarding and Vulnerable Groups Act (2006)

Early Years Foundation Stage Statutory Framework (2024)

#### Further Guidance

Working Together to Safeguard Children (2023)

What to do if you are worried a Child is Being Abused (HMG 2015)

This policy was adopted at a meeting of Crestwood Pre-school Committee

Held on \_\_\_\_\_ Date to be reviewed \_\_\_\_\_

Signed on behalf of the management committee \_\_\_\_\_

Name of signatory \_\_\_\_\_

Role of signatory\_\_\_\_\_.