

**Beaumont Community Preschool & Childcare Groups**

**Online safety (Inc. mobile phones, smartwatches and cameras)**

**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 and the use of mobile phones, smart watches, cameras, tablets and videos

**Procedures**

* Our designated persons responsible for co-ordinating action taken to protect children are:

**Nicole Breakwell and Kate Vass**

***Information Communication Technology (ICT) equipment***

* Only ICT equipment belonging to the setting is used by staff and children.
* The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
* All computers have virus protection installed.
* The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

***Internet access***

* Children do not normally have access to the internet and never have unsupervised access.
* If staff access the internet with children for the purposes of promoting their learning, written permission 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.
* Staff complete online safety training.
* 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 safely.
* 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 or discrimination 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 their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or 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.
* Staff send any personal information and always share information securely.

***Mobile phones and smartwatches – 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 [lockers or a locked drawer] until the parent collects them at the end of the session.
* Children are not to wear smartwatches within the setting.

***Mobile phones and Smartwatches – staff and visitors***

* Mobile phones/smartwatches are either turned off or on silent and not accessed during working hours or for parents/visitors are not used on the premises whilst children are present.
* Mobile phones/smartwatches can only be used on a designated break and then this must be away from the children.
* Mobile phones/smartwatches should always be stored safely in staff lockers during the hours of your working day.
* 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 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/videos of children.
* Parents and visitors are requested not to use their mobile phones or any other recording devices including smartwatches 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.

***Cameras and videos***

* Our staff and volunteers must not bring their personal cameras or video recording equipment into the setting.
* Photographs and recordings of children are only taken on the settings own devices and are 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 onto social media sites such as Facebook/Twitter etc.
* 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.
* If staff/volunteers are friends with service users on social media, they must abide by Information Sharing and Confidentiality procedures, staff/volunteers must not at any time discuss the setting or children/families attending or any issues relating to the setting.
* In the event that staff/volunteers 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/volunteers should always maintain professionalism and 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/discussions, including on social networking sites, with the children and parents with whom they act in a professional capacity.
* Any member of staff; committee member; volunteer or student found to be posting remarks or comments that breach confidentiality and or are deemed to be of detrimental nature to the setting or other employees or posting/publishing photographs of the setting, children or employees without relevant consent may face disciplinary actions in accordance with Beaumont Community Preschool & Childcare Groups policies and procedures.
* The use of social networking sites during working hours is not permitted. Staff Members; committee members; volunteers and Students are made aware of our policy during the induction process.

***Electronic learning journals for recording children’s progress***

* Managers seek permission from the committee management team prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
* Staff always adhere to the guidance provided with the system .
* Please refer to Electronic Learning Journal and Data Protection policy and procedures for more detail.

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

* Staff are aware that it is an offence to 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).

|  |  |  |
| --- | --- | --- |
| This policy was adopted by |  | *(name of provider)* |
| On |  | *(date)* |
| Date to be reviewed |  | *(date)* |
| Signed on behalf of the provider |  | |
| Name of signatory |  | |
| Role of signatory (e.g. chair, director or owner) |  | |