

Policy regarding the use of mobile phones, electronic devices and cameras

This policy refers to all electronic devices able to send or receive calls and messages, take pictures and record videos. This includes mobile phones, cameras, tablets, recording devices and smart/fitness watches. Technology is changing all the time, and we will adapt this policy as required. Staff, visitors, volunteers and students are not permitted to use electronic devices to take or record any images of the children. Staff must only use the designated camera(s) whenever they are taking photographs in the setting. Parents need permission from the designated safeguard lead to use electronic devices for photographs, images or recording in the setting Procedures

- Under the Data Protection Act (2018) and GDPR, the setting must seek parental consent to take photographs/videos. The parent/carer of each child is required to complete a consent form which gives the reasons and specific purposes for photographs and images being taken (for example; 1. Consent for use of photos/video recorders for Learning diaries, 2. consent for use for Publicity and 3. consent for use for Settings website.)
- The setting has a designated camera (s) which is the responsibility of the staff.
- The information contained within each learning diary is to relate to an individual, identifiable child; therefore, it is to be treated as personal data.
- Images are to be stored in line with the Data Protection Act 2018 • As a setting we are registered with the Information Commissioners Office (I.C.O) for data protection and our registration number is Z2161056
- All images will be stored and disposed of securely. The aim will be to prevent unauthorised access, ensure confidentiality and protect identity.
- The following aspects of security are to be managed accordingly: 1. Physical security – effective measures will be put in place to ensure physical security and to protect against theft, including that of laptops, computers, cameras, and any personal data, including photographic images. 2. Computer security – effective measures are to be implemented to ensure computer security. Awareness will be raised in respect of technological advancements which could put online systems at risks.
- Security procedures are to be proportionate to the potential risks involved and must be subject to constant monitoring and review
- Photographs will be stored on the settings computer/laptop, which is password protected, in accordance with the setting's data retention schedule. When the images are no longer required or the setting ceases to operate, all photographs will be shredded or deleted from the computer or laptop.
- Photographs are printed in the setting by staff and images are then removed from the camera's memory.

- The practitioners are to ensure all photographs are permanently wiped from memory sticks/cards, computer hard disc and portable devices or other relevant devices once the images are no longer of use.

- Children have their photographs taken to provide evidence of their achievements for developmental records. Photographs may be taken during indoor and outdoor play and displayed in albums or a child's development record/learning diary for children and parent/carers to look through.

- Often photographs may contain other children in the background. If a parent/carer has not completed a consent form for the relevant usage, we will not use an image where that child appears in the background

- Events such as, sports day, outings, Christmas and fundraising events may be recorded by video and photographs taken by staff and parent/carers but always in full view of all attending. Parents/carers, staff, volunteers and students will be notified of this in advance. At the beginning of every event parents/carers, staff, volunteers and students will be reminded not to include photographs of children other than their own on social media.

- No images will be taken of children which captures them in what are commonly understood as non public activities like toileting or changing clothes, or which show body parts not usually visible in public settings.

- Use of cameras, electronic devices and mobile phones is prohibited in the toilet or nappy changing area.

- If photographs of the children taking part in an activity are used to advertise/promote our setting via our web site, in the local press etc; we do not show children who are in breach of rules or are behaving in a reckless or dangerous fashion.

- To encourage children's development (understanding the world; technology) children have supervised access to the settings tablets. Children take photographs and videos on the tablet and are fully supervised by staff members doing this.

- Passwords and codes for the setting devices must not be shared with anyone other than staff.

- We will do our up most to protect children's identity: We will not photograph children where consent is not given

Electronic devices belonging to staff, volunteers, students and others will be left in the designated secure area which is situated in the Office. These should be turned off/ on silent and not accessed during working hours other than break/lunch times and this must be away from the children.

- No electronic device is allowed to be connected to the setting WIFI at anytime. Smart and/or fitness watches can be worn if WIFI/ Bluetooth is off. Devices that only count steps/monitor health are permitted

- Personal calls must be directed through the settings phone.

- Staff must not make personal calls during their working hours. However, in urgent cases, a call may be made or accepted if deemed necessary and by arrangement with the Leader/Manager.

- The settings mobile phone is labelled as such and is kept in the desk drawer. The camera facility is not used.

- Visitors and parents can only use their phones outside the building unless they have received permission from the designated safeguard lead.
- Staff will be vigilant when children are in the outside area to prevent unauthorised persons taking photographs or recording images.

Policy Date:

Review Date:

Signed