

## Use of mobile phones, electronic devices and cameras

### Policy Statement

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.

Where a particular situation arises concerning a form of technology that has not been mentioned in this document, we trust that the safeguarding training of our staff will result in the appropriate action being taken to safeguard the children in our care.

**Staff, visitors, volunteers and students are not permitted to use personal electronic devices to take or record any images of the children. Staff must only use the designated cameras whenever they are taking photographs 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:
  1. consent for use of photos/video recorders for parental view of child's time at The Den,
  2. consent for use for publicity and
  3. consent for use for The Den website.
- The setting has 2 designated cameras, (one ipad and one iphone), which are the responsibility of the manager or deputy manager on shift and reportable to the designated safeguarding practitioner.
- 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 ZA112673
- 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:

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. The Den has a triple lock facility (front door, room door and cupboard door).

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. Photos stored on Google Drive with password protection at point of computer access and login to the drive.

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 and the encrypted memory stick.

- Security procedures are to be proportionate to the potential risks involved and must be subject to constant monitoring and review
- The setting's digital camera/s or memory cards must not leave the setting except to download by the owner and designated safeguarding officer (Anna Griffin) and will not be removed from the site electronically unless there is a specific reason which has been agreed with the designated safeguarding officer.
- In the case of an outing or other activity away from the setting, risks must be minimised, e.g. download all photos before removing camera/s or memory cards and other portable devices from the setting.
- 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 newsletters, online and for parent/carers to look through. This is only in accordance with parental consents.
- 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 and is clearly identifiable.
- It is acceptable to blur/cover a child's identity (face) when promoting an image.
- 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 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. These are set up with age appropriate games and apps. The tablets have restrictions to ensure we safeguard children and are checked regularly.
- Children are aware of the rules relating to use of the tablets. Children take photographs and videos on the tablet and are fully supervised by staff members doing this. Protocol in relation to storage of photographs will also be followed in relation to the tablets.
  - Children DO NOT have access to the internet on these devices
- Passwords and codes for the setting devices must not be shared with anyone other than staff.

- A breach of this policy could result in disciplinary action and staff allegations procedure will be followed.
- We will do our up most to protect children's identity: We will not photograph children where consent is not given.

## **Electronic devices**

### **Staff**

- Personal electronic devices should be turned off/ on silent and not accessed during working hours and this **must be away from the children**.
- Staff are permitted to have their mobile phone on them during the session however, must not make personal calls, check messages, use for personal use during their working hours. However, in urgent cases, a call may be made or accepted if deemed necessary and by arrangement with the shift manager.
- Staff are rigorously trained in safeguarding and are aware of their responsibilities to the children and use of their personal devices.

### **Volunteers**

- Personal electronic devices 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.
- Volunteer devices must be left in the designated secure area which is situated in The Den locked cupboard. 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.

### **Children**

- We are aware that a growing number of children now have a mobile phone/electronic device that connects to the internet, has a camera and has communication technology.
- Children must hand in all mobile phones/tablets at the start of the session. These will be stored in the designated secure lockbox which is situated in The Den locked cupboard. In the event of outside play the entire box must be brought outside.
- These should be turned off/ on silent and not accessed during the session.
- No electronic device is allowed to be connected to the setting WIFI at anytime.
- We will use our discretion with smart and/or fitness watches depending on their capability. If the device is able to take or make calls or messages, these are to be left in the designated lockbox OR disconnected during the session. Devices that

only count steps/monitor health are permitted

- Parents/carers are made aware that their children are not allowed to wear electronic devices such as i-watches that are connected during the session.
- Staff can request the turning off of the device or handing it in for safekeeping.

## Visitors and Parents

- Visitors and parents, if remaining on site must hand in their phone/technology as part of their sign in process.
- When collecting a child and whilst on site, parents should not have their phone out/in use. Parents must be aware that staff will ask them to put their phone away if it is in use whilst on site.

## Outside Play

- Staff will be vigilant when children are in the outside area to prevent unauthorised persons taking photographs or recording images.
- Staff must report and record any behaviour where they believe photographs have been taken as an incident and verbally alert the designated safeguarding officer.

[illegible]