CCTV Policy

1. Monitoring

a. The CCTV is monitored centrally from the nursery office and is registered with the Information Commissioner under the terms of the Data Protection Act. This policy outlines the nursery's use of CCTV and how it complies with the Act. The nursery complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly.

b. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained to understand their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

c. Surveillance camera system images and information are subject to appropriate security measures to safeguard against unauthorised access and use

d. Effective review and audit mechanisms are undertaken to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published

e. A copy of this CCTV Policy will be provided on request to staff, parents and visitors to the nursery and will be made available on the website and in the policy file

f. If CCTV images are reviewed following an incident or an allegation, a record is made. Under no circumstances are CCTV images shared with parents or other service users unless there is a legitimate reason for doing so, i.e. to disprove an allegation against a member of staff. The process for using CCTV in these circumstances is as follows:

- an allegation or incident occurs that may have been caught on CCTV
- setting manager reviews CCTV footage and retains a record
- if there is reason to believe that a crime may have been committed then an investigation takes place
- if a parent or other person whose image has been recorded and retained and wishes to access the images must apply to the setting manager in writing
- the Data Protection Act gives the manager the right to refuse a request to view the images, particularly where such access may prejudice the prevention or detection of a crime
- if access to the image is refused then the reasons are documented and the person who made the request is informed in writing within 28 days. The images are not destroyed until the issue is resolved

2. Location of Cameras

a. The location of CCTV cameras will be clearly indicated and adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation.

b. Adequate signage will also be prominently displayed at the entrance to the nursery's property.

c. CCTV cameras are not placed with a view into any private areas such as the toilet block or changing rooms.

3. Storage and Retention

a. The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. The images/recordings will be stored in a secure environment with a log of access kept.

b. No more images and information should be stored than that which is strictly required for the stated purpose of the surveillance camera system, and such images and information should be deleted once their purpose is discharged

c. Access is restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the manager. In certain circumstances, the recordings may also be viewed by other individuals. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

d. Only the setting manager, the owner and deputy have access to retained CCTV images. If an instance arises where the CCTV images need to be reviewed to prove or disprove an allegation or incident, this is the responsibility of the setting manager who will share the images with the police, social care or Ofsted to assist with an official investigation if required. A record is retained, containing the date of the incident/allegation; camera number of positions; brief description of the incident/allegation – with reference to related safeguarding forms; who the footage was viewed by, date viewed and action taken – and counter signed by a senior member of staff. Images may also be requested by the owners/directors/trustees for the purpose of conducting an investigation into an incident.

e. Under certain circumstances, the CCTV footage may be used for training purposes (including staff supervisions) or for parents to view child transitions.

4. Subject Access Requests (SAR)

a. Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act / GDPR. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

b. The nursery will respond to requests within 14 calendar days of receiving the request. The nursery reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation. A record of the date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) and why they required it will be made. Where footage contains images relating to 3rd parties, the nursery will take appropriate steps to mask and protect the identities of those individuals.

5. Responsibilities

The manager (or deputy) will:

a. Ensure that the use of CCTV systems is implemented in accordance with this policy

b. Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes

c. Ensure that all CCTV monitoring systems will be evaluated for compliance with this policy

d. Ensure that the CCTV monitoring is consistent with the highest standards and protections

e. Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy

f. Maintain a record of access (e.g. an access log) to or the release of files or any material recorded or stored in the system

g. Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally

h. Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals

i. Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of “Reasonable Expectation of Privacy”

j. Ensure that monitoring footage is stored in a secure place with access by authorised personnel only

k. Ensure that images recorded are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).

l. Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics