CONTROL OF RECORDS

This Policy summarises the systems and arrangements in place at the setting to control records and personal files in line with the requirements for OFSTED Registration, and the requirements of the latest edition of the ISO 9001 Quality Standard.

1. Each set of records will be maintained in a secure location within the setting's Administration offices, and in such a manner as to prevent deterioration or spoilage. Records will be collated and filed in an orderly fashion and indexed so as to be easily retrievable.

2. A Quality Records Log will be maintained which will identify the following for each set of records, taking into account statutory requirements as applicable:

   2.1 Location of storage.

   2.2 Disk References, where records are stored on word processor / computer.

   2.3 Length of time records are kept ("Retention periods").

   2.4 Responsibilities for maintenance and control.

   2.5 Restrictions on staff who are authorised to have access to individual sets of records.

3. Obsolete records will be processed as follows:

   3.1 Where history records are required - archived under the control of the setting Manager. In such cases, archiving shall be for an initial 5-year period, after which the Manager will review the need to continually retain the records. Thereafter, archived records will be reviewed annually; those that can be disposed of will be shredded, per 3.3 below.

   3.2 The setting Manager must always be aware of appropriate legislation / regulations governing the storage periods for archived records, and archiving will be in accordance with these requirements. A log of archived records will be maintained by the setting Manager.

   3.3 Disposal - by shredding. NB This will require written authorisation from
   the setting Management.

CCTV

4.3 Employees are not permitted to withdraw their labour in pursuit of grievances. Lily’s Kids Klub has in place a CCTV surveillance system across

various locations on the premises. Images are not monitored all the time but they are recorded centrally and will be used in strict accordance with this policy.

The system is owned by the setting. The setting Management team is responsible for ensuring this policy is implemented.

The setting Management team may be contacted as follows:

Bridget Nicol	Office	020 8674 8678	or	07958 346 058
Josephine Showers	Red Room	020 8674 8678	or	07983 626 627

Bridget Nicol (pre-school manager) is responsible for ensuring compliance with the policy and the procedures it contains.

DATA PROTECTION ACT 1998:

CCTV recording, if it shows a recognisable person, is Personal Data and is covered by the Data Protection Act. This policy is associated with the setting's Data Protection Policy, the provisions of which should be adhered to at all times.

1. THE SYSTEM

The system comprises 6 fixed position cameras, a monitor, digital hard drive recorder and 1 public information signs.

Cameras are located at strategic points on the premises, principally at the hallway, red room, blue room, learning room and the lower ground hall.

No camera is hidden from view and all will be prevented from focussing on areas of private accommodation. Signs are prominently placed at entrance and exit points of the site to inform staff, pupils, parents, visitors and members of the public that a CCTV installation is in use. The digital recorder and single monitor screen are located in the nursery office. Although every effort has been made to ensure maximum effectiveness of the limited system it is not possible to guarantee that the system will detect every incident taking place on the site.

2. PURPOSE OF THE SYSTEM

The system has been installed by the setting with the primary purpose of monitoring

- staff interaction with children
- ensure that children are appropriately cared for
- facilitate the identification of any activities / event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to the setting Manager.
- reducing the treat of a child being abducted
- damage to the building
- theft
- assist in the prevention and detection of crime;
- helping to ensure the safety of all the users, staff, pupils, parents and visitors, consistent with respect for the individual's privacy.
- Deter those having criminal intent
- Identify any activities which might warrant disciplinary proceedings being taken against staff, pupils, parents or visitors and assist in providing evidence

to the setting and to the individuals against whom disciplinary action is, or is threatened to be taken.

The system will not be used to: Provide images for the world-wide-web; Record sound.

3. THE DIGITAL RECORDER

Images captured by the system will be recorded and reviewed (in the event of an incident) at the location of the recorder and its monitor. The monitor will not be visible to staff who are not authorised to view the images. The VDU monitoring screen is turned off at the end of the working day. Access to the recording system will be strictly limited to the Management team, police officers and other individuals granted access on a case-by-case basis, with written authorisation from the Manager / Proprietor. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted by a member of the nursery management team, to persons with a legitimate reason to access the system. The identity of any visitor must be checked before access is allowed.

4. ADMINISTRATION AND PROCEDURES

The administration of the system is the responsibility of the Management team. It is recognised that images are sensitive material and subject to the Data Protection Act 1998; the Manager / Proprietor is responsible for ensuring day to day compliance with the Act. All recorded data will be handled in strict accordance with this policy and the procedures that form part of it.

5. STAFF

All staff involved with the CCTV system will be made aware of the sensitivity of handling CCTV images and recordings. The Manager / Manager will ensure that these individuals are fully briefed in respect of the operation and administration of the CCTV system.

6. RECORDING

Digital recordings are made using digital data to the hard drive supplied with the system. Incidents are recorded in real time. When the hard drive is full the system automatically overwrites the earliest recorded images. (This could be every month) The hard drive will be inspected annually, as advised by the suppliers, for surface defects. A log of such checks will be kept. Hard drives used will remain the property of the setting until disposal and destruction.

7. ACCESS TO IMAGES

All access to images will be recorded in the Access Log, as shown in the Appendix. Any visitor with the authority to access the images must complete and sign the Access Log. Access to images for staff other than those specified in 3 is restricted to that staffs that needs to have access in accordance with the purposes of the system. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and in compliance of the Data Protection Act 1998, after a correctly
authorised and served documentation is received. Such access will be limited to:

- Law enforcement and government agencies where images recorded would assist in a criminal enquiry or the prevention of terrorism and disorder;
- Prosecution agencies;

- Relevant legal representatives;
- The media, where the assistance of the general public is required in the identification of a victim or a perpetrator of a crime;
- People whose images have been recorded and retained unless such disclosure would prejudice criminal proceedings;
- Emergency services in connection with the investigation of an accident.

8. ACCESS TO RECORDINGS BY A DATA SUBJECT

Anyone who believes they have been filmed by a CCTV system is entitled to ask for a copy of the recording, subject to the prohibitions on access also covered by the Data Protection Act 1998. They must apply in writing to the Data Protection Officer, the request being accompanied by the fee of £100.00. A response will be provided promptly and in any event within twenty eight days of receiving the fee and the request. The Data Protection Officer has the right, according to the Act, to refuse a request for a copy of the images, particularly where such access could prejudice criminal proceedings.

9. REQUEST TO PREVENT PROCESSING

An individual has the right to request the prevention of processing where this is likely to cause substantial and unwarranted damage to that person. Requests should be addressed to the Manager, who will provide a written response within 21 days, setting out their decision. Copies will be kept of the request and the decision.

10. COMPLAINTS

Should members of the setting have concerns or complaints about the operation of the system, they may follow the setting's Complaints Procedure, initially addressing their complaint to the Manager. Concerns relating to the Data Protection Act 1998 should also be addressed to the Manager. These rights do not alter the existing rights of members of the setting, or any other individuals under any relevant grievance or disciplinary procedures.

11. COMPLIANCE MONITORING

Upon request to the Management team, enquirers will be provided with:
- A copy of this policy
- A copy of the Complaints Procedure

The effectiveness of the system in meeting its purposes will be kept under review.

12. CCTV SYSTEM

A list of the basic system checks required is detailed below:
- Checked (Date)
- By
- Date of
- Next Review

Notification of the system has been submitted to the setting and the next review date recorded. Cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime. Cameras have been positioned to avoid capturing images of persons not visiting the premises.

There are signs showing that a CCTV system is in operation visible to visitors to the premises. Contact details for the service provider are displayed. The recorded images from this CCTV system are securely stored, where access to them is limited to authorised persons only. The recorded images will only be retained until the system

writes over them. Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties. The operating equipment is regularly checked to ensure that it is working properly and that the date and time are correctly set. The Management team knows how to respond to requests from individuals for access to images relating to that individual.

APPENDIX **ACCESS LOG**

Name of Applicant……

Reason for Application for Access……

……

……

……

……

……

……

Date received……

Fee received……..

Signature of Applicant……

Access granted (Date and By Whom) …….

……