THE USE OF CCTV CAMERAS - POLICY & PROCEDURE

APPLICATION

Muddy Puddles Nursery recognises that both covert and overt surveillance can have legitimate uses. However, laws must be followed to ensure that any benefits of CCTV are weighed against the impact on a person's privacy. The use of CCTV in nursery settings is likely to raise greater privacy concerns than in any other kind of business, due to the nature of the care being provided.

Children's privacy and dignity are paramount to Muddy Puddles Nursery. This policy aims to ensure that, when CCTV is considered and implemented, there is an appropriate balance between protecting children from harm and ensuring that the privacy rights of children, staff, families, and visitors are respected.

All Sites must follow this policy when deciding to implement CCTV systems and when collecting, storing, processing and sharing CCTV footage.

This policy should be read in conjunction with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice, both of which must be adhered to at all times.

PURPOSE

The purposes of this policy are as follows:

- To protect children, staff and visitors
- To set acceptable parameters for the use of Safety Monitoring and ensure that any CTTV system is not abused or misused.
- To ensure compliance with the Home Office Surveillance Camera Code of Practice and the ICO CCTV Code of Practice.
- To support the Sites in meeting the provisions expected under the Early Years

Key Question	Key Lines of Enquiry
Quality of education	How are risks to people assessed and their safety monitored and managed, so they are supported to stay safe and their freedom is respected?
Behaviours and attitudes	How are people's privacy, dignity, independence respected and promoted?
Personal development	How are people's concerns and complaints listened to, responded to, and used to improve quality of care and education?
Leadership and management	Does the governance framework ensure that responsibilities are clear, and that quality performance, risks and regulatory requirements are understood and managed?

	Is consent to care and treatment always sought in line with legislation and guidance?
	How do systems, processes and practices keep people safe and safeguarded from abuse?

- To meet the legal requirements of the laws and regulations that the Sites are subject to, including the following:
- Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interpretation of Communications) Regulations 2000
- Education Act 2005
- Education and Skills Act 2008
- Education and Inspections Act 2006
- Childcare Act 2006
- Freedom of Information Act 2000
- Human Rights Act 1998
- Protection of Freedoms Act 2012 (links to) The Protection of Freedoms Act 2012 (Disclosure and Barring Service Transfer of Functions) Order 2012
- General Data Protection Regulation 2016 (GDPR)
- Data Protection Act 2018 (DPA)

SCOPE

The following roles may be affected by this policy:
- ALL TEAM MEMBERS

The following people may be affected by this policy:
- CHILDREN

The following stakeholders may be affected by this policy:
- FAMILY MEMBERS
- VISITORS
- EXTERNAL HEALTH PROFESSIONALS
- LOCAL AUTHORITY

OBJECTIVES

The objectives of this policy are as follows:
- To ensure that CCTV is operated lawfully and only for the defined purposes set out in this policy.
- To ensure that the rationale for the use of CCTV is clear and that CCTV is only used where required in order to:
- Ensuring the safety and well-being of children
- Monitoring the activities of team members
- Managing and monitoring of quality standards
- Ensuring public safety
- Protecting children and team members
- Protecting team members from allegations or assault or improper behaviour
- To ensure that the Sites have due regard for the privacy of all children, staff and visitors.

- To ensure that staff, children, relatives and visitors understand their rights regarding the use of CCTV equipment within the Sites.

POLICY

Muddy Puddles Nursery recognises and endorses people's right to privacy and dignity whilst balancing this with the need for protection from harm or danger.

Where CCTV is being introduced into an existing Site with current children, Muddy Puddles Nursery considers it is best practice to consult with, and obtain consent from, residents, families and visitors for the use of CCTV. For new Sites, or where CCTV has already been introduced into a Site, express consent will not generally be required from residents/families/legal representatives. The Site should make it clear to children's families that CCTV will be in use to enable them to make an informed choice about whether to choose the Site. The Site should always consider, in particular circumstances, whether consultation with, or consent from, new children is required expressly from their parent/ guardian.

The Sites will have a designated Data Protection Officer (DPO) who will take legal responsibility for the operation and compliance of the CCTV system and resulting data. At the Site this is Mayur Somaiya who is also the DPO for Muddy Puddle Nursery. The Sites will adhere fully to the 12 principles of the ICO CCTV Code of Practice.

The storage and disclosure of information from CCTV systems will be controlled and consistent with the purpose(s) for which the system was established and in line with data protection principles.

The use of CCTV will never substitute suitably skilled, knowledgeable staff in relation to the numbers required to support children. Where the delivery of poor care is identified with safety monitoring equipment, relevant policies will be followed. Where criminal activity is discovered or suspected, the Sites will notify relevant authorities and bodies e.g. Police.

Images monitored and recorded via the CCTV systems will be used in strict accordance with this policy.

PROCEDURE

PRIVACY IMPACT ASSESSMENTS

- The Site will conduct a Privacy Impact Assessment (PIA) in line with its GDPR policy on PIAs before considering any CCTV System or modifying an existing system.
- If the PIA identifies high risks to privacy that cannot be mitigated, prior consultation must take place with the ICO before the CCTV system can be utilised.

SITING OF CCTV SYSTEMS

- Authorisation must be obtained from Muddy Puddles Nursery before introducing a new CCTV System or modifying an existing one.
- CCTV equipment may be installed in all communal areas of the building where the Site has determined that this is justified in accordance with the PIA. CCTV must not be installed in communal bathrooms or toilets.

TRANSPARENCY

- Transparency and openness about the use of CCTV are vital to meet legal requirements and to retain the trust of children, families, and visitors. For this reason, except in exceptional circumstances, only overt surveillance may be used.

- Appropriate signage will be displayed at all areas of the Site where CCTV systems are being used with prominent notices at main entrances to the Site and next to the visitor signing in the book so as to notify those entering the building that they may be monitored by CCTV systems.

- The signs must be clearly visible and readable and will contain details of the organisation operating the CCTV systems (being the Sites Data Controller), the purpose of CCTV, the CCTV cameras log and who to contact about the CCTV systems. The signs will direct readers to where they can access a more detailed CCTV privacy notice that complies in full with the transparency requirements of the GDPR.

- There may be very limited circumstances where the use of covert surveillance is appropriate and legitimate, for example where this is required to obtain evidence of poor care in the interests of ensuring safe, high-quality care for residents. Covert surveillance should be treated with extreme caution and only used in the most exceptional of circumstances when all other means of achieving the same purpose have been considered. The Site should take advice from the DPO on any proposed use of covert surveillance.

MONITORING

- When viewing is carried out by the Site, that review will be carried out by authorised persons and a list of authorised persons will be maintained by the Site. All viewing of images will be recorded on the Footage Review Log including the names and descriptions of those present.

- In order to ensure child safety, a system of random monitoring of images will take place where there has not been any alert or cause for concern. This will be done proportionately to minimise the impact on the child's privacy, and that area within the building will not be subject to persistent or targeted monitoring where there has been no alert or cause for concern. The Site will determine how often monitoring will take place and how much footage will be monitored and will record this in the Site's PIA. Random monitoring will be carried out by an authorised, senior member of staff.

RECORDINGS

- All recordings shall remain the property of the Site until disposal and destruction.

QUALITY OF IMAGES

- Images produced by the equipment should be clear in order that are effective for the purpose/s for which they are intended. For example, if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for the purpose.

- Camera installation should be undertaken by NSI approved security companies, under appropriate service contracts, where the equipment is placed in or on the site of the premises at the Sites. Upon installation, all equipment must be tested to ensure that only the designated areas are monitored and that high-quality pictures are available in live and playback mode.

- All CCTV equipment should be serviced and maintained on an annual basis by an NSI approved company. The Site should have access to the manufacturer's guidelines for the system in use.

- The system can consist of cameras recording to digital recorders. These recorders must be in a secure location. Access (including both access to the secure location in which the recorders are stored and access to electronic images) must be limited to only those individuals named as Authorised Individuals in this policy.

PROCESSING IMAGES

- CCTV images, should not be retained for longer than is necessary for the purpose/s of which the equipment is being used. While images are retained, it is essential that their integrity is maintained, whether it to ensure their evidential value or to protect the rights of people whose images may have been recorded.
- Images should be deleted automatically after 30 days. The Site should record this in the PIA and monitor to ensure that the images are, in fact, being deleted after this period of time.

DAY TO DAY OPERATIONS

- Whilst the CCTV system will be constantly recording images the viewing system will not be in live viewing mode.

- The viewing system will only be put into live mode if an accident or incident is reported and data needs to be obtained to enable further investigations to be completed. In this instance, the general manager and/or duty manager will be contacted, and they will access the viewing system to view the event to obtain relevant data. The Viewing Log Record will be completed to show that the footage has been viewed by the general manager and/or duty manager as appropriate.

- In the event of that the information needs to be shared with the emergency services or any other third party, then this will be authorised by the general manager and/or duty manager in accordance with the section headed “Access to images by third parties” below. The Viewing Log Record will be completed to show that the footage has been viewed by/shared with the relevant third party. If the relevant third party requires the Site to retain the CCTV footage for longer than the Site’s usual retention periods to assist in the investigation, the footage will be stored securely and separately from other footage until the investigation is completed or an earlier date if it is confirmed that the footage can be deleted earlier.

ACCESS TO IMAGES BY THIRD PARTIES

The Sites will make disclosures to third parties only in strict accordance with the purposes of the CCTV systems and with this policy, and only where allowed by law, in particular data protection law. Such disclosures are limited to the following organisations/individuals:

- Law enforcement agencies where footage may help in a criminal enquiry or with the prevention and/or detection of crime.
- Regulatory bodies (such as OFSTED who regulate facilities or the ICO which regulates the use of personal data).
- Prosecution agencies e.g. police
- Legal representatives
- Relatives or carers of children where such individuals have expressed concern about the care and treatment of a child or where the child’s parent or guardian has given consent for a relative to have access.
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings

- Emergency services in connection with the investigation of an accident or incident e.g. ambulance service.

In all cases where access to images is requested by a third party, the following procedure should be follows:

- A written request should be obtained from the third party.
- Checks should be carried out to ensure that the third party is legitimate and to verify the identity of the requestor.
- The request should be assessed to determine whether the images can be disclosed to the third party in compliance with the GDPR and the DPA.
- Only the minimum amount of footage should be disclosed to the third party to enable the third party to fulfil the purposes of the request.
- The Site should consider whether images of certain individuals should be obscured, for example if the footage contains images of individuals who are not relevant to the request.

ACCESS TO IMAGES BY A DATA SUBJECT

CCTV digital images, if they show a recognisable person, are personal data and are covered by the data protection legislation including the GDPR. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of images of them, subject to various exemptions, the most common of which are set out below. A request by an individual for a copy of images of them is a "subject access request".

A person who wishes to access images of themselves can make a request to anyone in the Site in writing or verbally. The Site can encourage individuals to use the Access Request Form but any request made will be valid. The Site must therefore ensure that all staff are trained to recognise and escalate subject access requests. No fee is payable.

It is permitted for the Site to ask the person requesting to see CCTV footage to provide as much detail as possible to identify themselves (e.g. hair colour, clothing worn etc. and about the time and location that the images were recorded) and proof of identity.

All valid subject access requests will be dealt with as soon as possible and within one month of receipt.

The DPA gives the Site the right to refuse a request for a copy of the data in limited circumstances, the most common of which are where such access:

- would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders; or
- would identify another person whose consent to disclosure has not been obtained, however the Site should consider whether it can provide images that include another person. This will be possible if the image of the third party can be sufficiently obscured or if it is reasonable to disclose the image of the third party (for example, the third party is in a communal area and is not doing anything particularly embarrassing). To respect the subject access rights, the ICO will expect the Site to look into options for obscuring third party images before refusing a request.

If is it decided that a subject access request is to be refused the reasons will be fully documented and the data subject informed in writing stating the reason/s.

COMPLAINTS

It is recognised that children, visitors, team members and others may have concerns or complaints about the operation of the CCTV systems. Any complaint should be addressed in the first instance to the general manager of the relevant Site. If the complaint remains unresolved after 28 days, the complainant if an employee should follow the grievance procedure and in any other case should refer their complaint to the directors of the Site. The Site must make the complaints procedure clear and easily available to all individuals.

COMPLIANCE MONITORING

The contact point for members of the public wishing to enquire about the CCTV systems will be the general manager of the Site.

Upon request enquirers will be provided with:

- A summary of this statement of policy
- An access request form if required or requested (for access to others' personal data)
- A subject access request form if required or requested (for access to their own personal data)

The general manager will seek input from the DPO or other senior Muddy Puddles Nursery employees if required in relation to any enquiry or complaint.

The general manager will be responsible for ensuring that the Site's record keeping in relation to the use of CCTV Systems complies with the requirements of the GDPR and that the Site has at all times accurate and up to date records in the event of an inspection by OFSTED.

REVIEW AND EVALUTION

The use of CCTV systems within the Site will be reviewed yearly alongside the ICO registration renewal requirement, or when opportunities to use alternative measures arise. The PIA will be reviewed at the same time and updated if required.

Feedback will be gathered from stakeholders, team members and residents in relation to the use of surveillance and this will be used to review practice and acted upon accordingly.

The Site will make use of the resources and audit tools available through the ICO as a means of assuring best practices in relation to surveillance systems.

The DPO must have a system in place to ensure that the date and time stamp recorded on images is accurate.

BREACH AND ENFORCEMENT

Where a personal data breach takes place, the Site will record this and will determine, with the Data Protection Officer, whether the Site should inform the ICO and/or the affected data subjects. A "personal data breach" is a breach of security that leads to unauthorised or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (i.e. images of individuals in CCTV footage). A personal data breach could be, for example, the corruption of a CCTV system, a hacking attack on the system or the loss of a disc containing CCTV footage.

The ICO has the power to issue enforcement notices. An enforcement notice will set out the remedial action that the ICO requires of the Site to ensure future compliance with the requirements of the GDPR and

the DPA. The ICO also has the power to issue significant fines of up to €20million for serious breaches of the GDPR.

Team members should refer to the GDPR Breach Notification Policy and Procedure and should escalate any breaches they become aware of in accordance with that policy.

The Site will complete the CCTV Data Protection Self-Assessment as provide by the ICO in order to gain assurance of full compliance with legislation, regulation and best practice.
Only staff who have been trained and have updated knowledge of the law relating to the use of surveillance and audio/visual equipment will be involved in any part of this policy and its associated procedures.

SURVEILLANCE BY OTHERS WITHIN THE SITE
Individuals within the Site may, from time to time, request additional surveillance to be carried out. The general manager will ensure that any concerns, and the reasons for requesting surveillance, are discussed and will attempt to resolve such concerns without resorting to surveillance. Where concerns discussed have the potential to be safeguarding issues, the safeguarding and regulatory bodies of the Site's relevant county council must be informed immediately.

Requests by individuals for surveillance must not be actioned unless the request is justified. The Site will complete a PIA and will work with the individual requesting the surveillance to implement alternative resolutions. The county council safeguarding team's advice will also be sought if the Site is concerned that the individual may proceed with surveillance without permission or if the situation becomes untenable.

Where the use of surveillance is justified, as demonstrated by the PIA, permission for surveillance must be sought from the individual to whom the concerns relate. A written plan must be in place detailing who will have access to the recordings, who they will be shared with and anything else that has been agreed in respect of the surveillance.

If unauthorised surveillance equipment is discovered in use, the general manager must be informed immediately, and all staff must be trained to inform the general manager. The following process will be followed:

- The general manager will, carefully and without damaging the equipment, turn off the device and remove it from the room, placing the item in a locked cupboard until the general manager can return it safely to its owner. The content will not be deleted.
- The general manager will take steps to identify who placed the recording equipment and investigate their reasoning for doing so.
- All parties involved will be informed that they have been recorded and informed of their rights, with appropriate support and advice from the Site.
- The Site will review any findings from the recording and will consider whether it is appropriate in the circumstances to act upon and investigate the findings, or to notify the county council safeguarding teams and/or OFSTED.
- Once the situation has been resolved, the general manager will agree with the person who initially used the surveillance how to proceed without the use of further surveillance and will warn that person that further surveillance without the permission of staff or relevant parent or guardian could result in a breach of the individual's terms and conditions or other legal and regulatory breaches.
- At no time will the care of any child be affected.
- Written records will be kept of the incident and resulting action.

RESPONSIBILITIES

The general manager is responsible for the day to day operation of the CCTV systems and for ensuring compliance with this policy.

The effectiveness of the CCTV systems in meeting their purposes and all documented procedures will be kept under review by the general manager.

This will involve ensuring that:

- There is a regular maintenance regime in place to ensure that the CCTV systems continue to produce high quality images.
- Regular checks are made that date and time stamps recorded on images are accurate.
- Regular consideration is given to whether the use of CCTV is still proportionate and justified or whether there is no longer a justifiable need for CCTV systems to be in use.

DEFINITIONS

As well as the terms that are defined throughout the policy, where the following terms are used in this policy, have the following meanings:

AUTHORISED INDIVIDUALS	▪ Nursery Manager ▪ Assistant / Deputy Manager
CONSENT	▪ A person's agreement to, or permission for a proposed action, particularly any form of examination, care, treatment or support ▪ Consent should be informed – the individual should know what they are consenting to because they understand the question and what it is regarding.
OVERT SURVEILLANCE	▪ This is where the individual being monitored would reasonably be aware of the surveillance occurring. For example, the use of a visible CCTV camera with clear signs stating that CCTV cameras are in use.
COVERT SURVEILLANCE	▪ Covert surveillance is where people being monitored would not be aware of the surveillance occurring, for example, a hidden CCTV camera.
SURVEILLANCE SYSTEMS	Surveillance systems are the technology and equipment used to carry out surveillance or to store and process the information gathered. Advances in technology mean that new systems or methods may become more common place. For simplicity in this information, we will generally make reference to surveillance which could encompass CCTV, Wi-Fi Cameras, audio recording, radio frequency identification (FRID) tracking and many other types of systems. This information sets out consideration's that can be applied to these and other existing or emerging technologies (CQC Definition)