

Our visions and values:

- Protecting children's right to play learn and have a voice.
- Keeping parents involved in children's development
- Governors and staff leading the way on quality
- Working partnership with health professionals and schools
- Being ethical, respectful and tolerant

CCTV policy

Status	Non-statutory
Responsible governors	Premises committee
Last review date	Spring 2024
Date of next review	Spring 2025
The policy is available for staff at:	School offices and shared drive
And for parents/carers at:	On request from school offices

Policy audit

Version	Revision date	Revised by	Section revised
V1	Spring 2021	Hasina Rashid	No changes
V2	January 2022	Alison Emmett	formatting
V3	January 2023	Alison Emmett	No changes
V4	January 2024	Hasina Rashid	No changes

Approval for premises committee

Name	Signature	Role	Date

1. Policy Statement

- 1.1. Church Hill and Low Hall Nursery Schools uses Close Circuit Television (**CCTV**) within the premises of the School. The purpose of this policy is to set out the position of the School as to the management, operation and use of the CCTV at the School.
- 1.2. This policy applies to all members of our workforce, visitors to the School premises and all other persons whose images may be captured by the **CCTV** system.
- 1.3. This policy takes account of all applicable legislation and guidance, including:
 - 1.3.1. General Data Protection Regulation ("**GDPR**")
 - 1.3.2. Data Protection Act 2018 (together the Data Protection Legislation)
 - 1.3.3. CCTV Code of Practice produced by the Information Commissioner
 - 1.3.4. Human Rights Act 1998.
- 1.4. This policy sets out the position of the School in relation to its use of CCTV.

2. Purpose of CCTV

- 2.1. The School uses CCTV for the following purposes.

- 2.2. To provide a safe and secure environment for pupils, staff and visitors
- 2.3. To prevent the loss of or damage to the School buildings and/or assets.
- 2.4. To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.

3. Description of system

- 3.1. The Cameras are Hikvision fixed 2MP HD Colour / mono Dome cameras without sound these cameras are fixed. The recorder is an Hikvision 8way HD DVR with 4TB hard drive

4. Siting of cameras

- 4.1. All CCTV cameras are sited in such a way as to meet the purpose for which the CCTV is operated. Cameras are sited in prominent positions where they are clearly visible to staff, pupils and visitors.
- 4.2. Cameras are not sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The School will make all reasonable efforts to ensure that areas outside of the School premises are not recorded.
- 4.3. Signs are erected to inform individuals that they are in an area within which CCTV is in operation.
- 4.4. Cameras are not sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

5. Privacy Impact Assessment

- 5.1. Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the School to ensure that the proposed installation is compliant with legislation and ICO guidance.
- 5.2. The School adopts a privacy- by- design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6. Management and access

- 6.1. The CCTV system is managed by the Business Manager and on a day to day basis the CCTV system is operated by the Site Services Officer.
- 6.2. The viewing of live CCTV images is restricted to Head Teacher, Business Manager, and Site Services Officer.
- 6.3. Recorded images which are stored by the CCTV system will be restricted to access by Head Teacher, Assistant Head Teachers in the Head Teacher's absence or the Business Manager.
- 6.4. No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.
- 6.5. The CCTV system is checked WEEKLY by the Site Officer or Business Manager to ensure that it is operating effectively

7. Storage and retention of images

- 7.1. Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

- 7.1. Recorded images are stored only for a period of 30 days unless there is a specific purpose for which they are retained for a longer period.
- 7.2. The School ensures that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
 - 7.2.1. **CCTV** recording systems being located in restricted access areas;
 - 7.2.2. The **CCTV** system is password protected;
 - 7.2.3. Restriction of the ability to make copies to specified members of staff
- 7.3. Executive Headteacher and Business Manager
- 7.4. A log of any access to the **CCTV** images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the School.

8. Disclosure of images to data subjects

- 8.1. Any individual recorded in any **CCTV** image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images.
- 8.2. Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the School's Subject Access Request Policy.
- 8.3. When such a request is made the Head Teacher, or the Business Manager will review the **CCTV** footage, in respect of relevant time periods where appropriate, in accordance with the request.
- 8.4. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Head Teacher or Business Manager must take appropriate measures to ensure that the footage is restricted in this way.
- 8.5. If the footage contains images of other individuals, then the School must consider whether:
 - 8.5.1. the request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals
 - 8.5.2. the other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained
 - 8.5.3. if not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- 8.6. A record must be kept, and held securely, of all disclosures which sets out:
 - 8.6.1. when the request was made
 - 8.6.2. the process followed by Head Teacher or Business Manager in determining whether the images contained third parties
 - 8.6.3. the considerations as to whether to allow access to those images
 - 8.6.4. the individuals that were permitted to view the images and when

8.6.5.whether a copy of the images was provided, and if so to whom, when and in what format.

9. Disclosure of images to third parties

- 9.1. The School will only disclose recorded **CCTV** images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
- 9.2. **CCTV** images will only be disclosed to law enforcement agencies in line with the purposes for which the **CCTV** system is in place.
- 9.3. If a request is received from a law enforcement agency for disclosure of **CCTV** images then Head Teacher, Business Manager and Site Services Officer must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the **CCTV** images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.
- 9.4. The information above must be recorded in relation to any disclosure.
- 9.5. If an order is granted by a Court for disclosure of **CCTV** images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10. Review of policy and CCTV system

- 10.1. This policy will be reviewed ANNUALLY
- 10.2. The **CCTV** system and the privacy impact assessment relating to it will be reviewed ANNUALLY

11. Misuse of CCTV systems

- 11.1. The misuse of **CCTV** system could constitute a criminal offence.
- 11.2. Any member of staff who breaches this policy may be subject to disciplinary action.

12. Complaints relating to this policy

- 12.1. Any complaints relating to this policy or to the **CCTV** system operated by the School should be made in accordance with the School Complaints Policy.

_____ End _____

CCTV PRIVACY IMPACT ASSESSMENT TEMPLATE

1. Who will be captured on **CCTV**?

Pupils, staff, parents/carers, volunteers, governors, contractors and other visitors including members of the public

2. What personal data will be processed?

Facial images, behaviour.

3. What are the purposes for operating the **CCTV** system? Set out the problem that the School is seeking to address and why the **CCTV** is the best solution and the matter cannot be addressed by way of less intrusive means.

Safeguarding of our school community including the children, staff and parents. Prevention or detection of crime etc.

4. What is the lawful basis for operating the **CCTV** system?

Legal obligation, legitimate interests of the organisation to maintain the safeguarding of all, the health and safety of all and to prevent and investigate crime.

5. Who is/are the named person(s) responsible for the operation of the system?

Head Teacher: Helen Currie
Business Manager: Hasina Rashid
Site Services Officer

6. The **CCTV** system:

Has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained.
Has cameras sited in locations that can capture vulnerable parts of the school to ensure the security of the school building and the safeguarding of our school community.
Has cameras that have been sited to avoid capturing images which are not necessary for the purposes of the **CCTV** system.
Signs notify individuals that **CCTV** is in operation.

7. Set out the details of any sharing with third parties, including processors

With third parties who are directly involved in dealing with any request, enquiry, complaint or other correspondence submitted by an individual which the footage is relevant to.
With third parties who are providing a school with professional advice with the footage is relevant to where necessary for their legitimate interests and permitted by law.
In line with Data Sharing agreement with the Metropolitan Police.
Where a school is legally required to do so, in connection with criminal investigations, legal proceedings or prospective legal proceedings which the footage is relevant to where necessary for the related legitimate interest of the school or a third party permitted by law.

To establish, exercise or defend a school's legal rights where necessary for their legitimate interests and permitted by law

8. Set out the retention period of any recordings, including why those periods have been chosen

30 days

9. Set out the security measures in place to ensure that recordings are captured and stored securely

Monitoring equipment is located in the server room and on the business manager's PC and Phone which is staffed at all times during school hours and locked outside of work hours. The equipment is password protected and only accessible via the schools secure network.

10. What are the risks to the rights and freedoms of individuals who may be captured on the **CCTV** recordings?

Risks to individuals' privacy in line with GDPR .
Risks around excessive data capture.
Risks around the system being unlawfully accessed.
Potential Data Breach risks.
Risks around disclosure to third parties or transfer of recordings.
Risks around Data Security.

11. What measures are in place to address the risks identified?

Ensuring that processing of recording is carried out fairly and lawfully – notices & CCTV policy in place.
Ensuring that any unnecessary footage captured will be securely deleted from the school system. Retention period.
Necessary security measures are in place to prevent any unlawful system access; the system is kept in a restricted area, use of encryption, individual passwords; access to system limited to specific personnel.
Data Breach risks are low as adequate security measures are in place to safeguard access to security system and data is deleted from the system entirely after 8 days.
Transfer risks are low – Police will attend site to view footage and do a physical download onto a secure device.

Data security risks are low as adequate security standards have been applied to the system (Anti-virus / firewall / Encryption/ Passwords) – live viewing of images restricted to limited personnel.

12. When will this privacy impact assessment be reviewed?

Annually

Approval:

This assessment was approved by the Data Protection Officer:

13. DPO

Date