

Muscliff Primary School

CCTV Policy



Approved by:	Senior Leadership Team	Date: November 2021
Last reviewed on:	November 2021	
Next review due by:	November 2024	

1. INTRODUCTION:

This document sets out the appropriate actions and procedures which must be followed to comply with the Data Protection Act in respect of the use of CCTV surveillance systems managed by Muscliff Primary School. Muscliff Primary School is registered with the Information Commissioners Office (ICO).

In drawing up this policy, consideration has been given to the following:

- The Data Protection Act 1998
- The CCTV Code of Practice produced by the Information Commissioner
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act 2000
- Caldicott Report 1997

The Data Protection Act 1998 came into force on the 1st March, 2000 and contains broader definitions than those of its predecessor (1984) Act and more readily covers the processing of images of individuals caught by CCTV cameras. The changes in data protection legislation mean that for the first time legally enforceable standards will apply to the collection and processing of images relating to individuals.

An important new feature of the legislation is the CCTV Code of Practice which sets out measures which must be adopted to comply with the Data Protection Act 1998. This goes on to set out guidance for the following of good data protection practice. The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.

2. SCOPE:

This policy will cover all employees of Muscliff Primary School, persons providing a service to the School, pupils, parents, visitors and all other persons whose image(s) may be captured by the system.

3. DEFINITION:

Prior to considering compliance with the principles of the Data Protection Act, a user of CCTV or similar surveillance equipment will need to determine two issues:

- a. The type of personal data being processed i.e. is there any personal data which falls within the definition of **sensitive personal data** as defined by Section 2 of the Act:

Sensitive personal data includes:

- Gender

- Ethnic origin or race
- Political opinion
- Religious belief
- Trade Union membership
- Health – mental or physical
- Sexual life
- Commission of any offence (or alleged offence)
- Any court proceedings or findings

b. The purpose(s) for which both personal and sensitive data is being processed. The data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individual's rights
- Secure
- Not transferred to countries without adequate protection

The Information Commissioner will take into account the extent to which users of CCTV and similar surveillance equipment have complied with this Code of Practice when determining whether they have met their legal obligations when exercising their powers of enforcement.

4. **POLICY APPLICATION:**

a. Initial Assessment Procedure

The Head Teacher of Muscliff Primary School has the legal responsibility for the School's CCTV systems. However, the School IT Manager has responsibility for the day-to-day compliance with the requirements of the CCTV Code of Practice. The Data Controller is Muscliff Primary School and the Data Controlling Officers are the Head Teacher, School Business Manager and the IT Network Manager.

The purpose of the School's CCTV scheme is for the:

- Prevention or detection of crime or disorder
- Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)
- Protection of School property and assets

Prior to any camera installation the IT Manager will ensure that the installation complies with the Data Protection Act and CCTV Code of Practice.

b. Siting the Cameras

It is essential that the location of the equipment be carefully considered because the way in which images are captured will need to comply with the Data Protection Act.

All cameras are located in prominent positions within public and staff view and do not infringe on neighbouring properties. All CCTV surveillance is automatically recorded and any breach of these Codes of Practice will be detected via controlled access to the system and auditing of the system.

Signs have been erected on all entrance points to the School's premises and throughout the site to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signs must include details on the purpose of the CCTV system that Muscliff Primary School is the Data Controller and provide contact details.

Use of Covert CCTV (Directed) surveillance if required should be requested through the Police. If the request through the Police is refused then authority can only be given by the Head Teacher. This is covered by the Regulation of Investigatory Powers Act 2000 (RIPA).

c. Quality of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme be clearly identified. For example, if a system has been installed to prevent and detect crime then it is essential that the images are adequate for that purpose.

All camera installations and service contracts should be undertaken by NSI approved security companies. Upon installation all equipment is tested to ensure that only the designated areas are monitored and high quality pictures are available in live and play back mode. All CCTV equipment should be serviced and maintained on an annual basis.

The system has 16 cameras recording to digital recording media. These cameras are currently monitored by the IT Manager through equipment located in the School office. The location of the cameras is listed at the end of section 9 of this policy.

d. Processing Images

Images which are not required for the purpose(s) for which the equipment is being used should not be retained. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that the access to and security of the images is controlled in accordance with the requirements of the 1998 Act.

- e. Recorded data will not be retained for longer than 31 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue. Where data is retained for longer than 31 days an

electronic file held on a secure central server where specific CCTV image/recordings are retained will be kept. The Data Protection Act and GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Therefore, retention will reflect the School's purposes for recording information, and how long it is needed to achieve this purpose. The School will store data securely at all times.

- f. Where the images are required for evidential purposes in legal proceedings a cd-r disc recording is made and placed in a sealed envelope, signed and dated and held in the School's main safe until completion of the investigation. Viewing of images within the School's office is controlled by the IT Manager or a person nominated to act on his/her behalf. Only persons trained in the use of the equipment and authorised by the IT Manager can access data.
- e. Access to and disclosure of images to third parties
It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled. This will ensure that the rights of individuals are preserved but also to ensure that the continuity of evidence remains intact should the images be required for evidential purposes eg. a Police enquiry or an investigation.

Access to the medium on which the images are displayed and recorded is restricted to School staff and third parties as detailed in the purpose of the scheme.

Access and disclosure to images is permitted only if it supports the purpose of the scheme. Under these conditions the CCTV images record book and the appropriate view/release form (see Appendix 1) must be completed.

- f. Subject Access Requests to images by individual,
Section 7 of the 1998 Data Protection Act gives any individual the right to request access to CCTV images.

Individuals who request access to images must be issued an access request form (See Appendix 2). Upon receipt of the completed form the IT Manager and the Business Manager – HR & Admin will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused.

A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons) within 21 days of receipt of the enquiry. If disclosure is appropriate a payment in advance of £10.00 will be required.

5. INTERACTION WITH OTHER SCHOOL POLICIES & PROCEDURES:

This policy should be read in conjunction with the School's Data Protection Policy.

6. ACCESS TO CCTV IMAGES

Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

7. RESPONSIBILITIES:

The Senior Leadership Team has corporate responsibility for the implementation of this policy, monitoring its effectiveness and ensuring the CCTV Code of Practice is available from the IT Manager.

We will ensure that the use of CCTV systems is implemented in accordance with this policy.

- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the School.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the School and be mindful that no such infringement is likely to take place.
- 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”
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Headteacher.

- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

6. ENFORCEMENT:

The Information Commissioner has the power to issue Enforcement Notices where he/she considers that there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice would set out the remedial action that the Commissioner requires of the School to ensure future compliance with the requirements of the Act.

7. DOCUMENTATION:

Copies of all documentation and records relating to the CCTV system will be held by the Business Manager. If a copy is taken from this, the Business Manager will need to keep this for a period of 6 years. All other recordings will be discarded.

8. ACCESS AND DISCLOSURE OF IMAGES TO THIRD PARTIES

There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police and service providers to the School where these would reasonably need access to the data (e.g. investigators). 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 School Business Manager should be contacted in the first instance and appropriate legal advice may be required. Requests for images should be made in writing to the School Business Manager. The data may be used within the School's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

10. REVIEW:

This policy will be reviewed every three years.

Camera locations:

- 1 Main Reception Area
- 2 Entrance lobby
- 3 Front entrance main car park

- 4 Playground/outside of Year 1
- 5 Outside by main gas meter
- 6 Broadway lane to playground passage way
- 7 Broadway lane to car park gate
- 8 Reception class playground
- 9 MUGA
- 10 Field/outside of Rainbow classroom
- 11 Field/outside of Rainbow classroom
- 12 Studio overlooking play equipment
- 13 Passage from main playground into school/extension end
- 14 Outside Whittaker Centre patio
- 15 Kitchen
- 16 Reprographics room

CCTV SIGNAGE

It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The School is to ensure that this requirement is fulfilled. The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded.
- The purposes of using CCTV.
- The name of the School.
- The contact telephone number or address for enquiries.

Example Sign



**WARNING CCTV
cameras in operation**

Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of the School and its property. This system will be in operation 24 hours a day, every day. These images may be passed to the police. This scheme is controlled by the School.