



Health, Safety
& Facilities

Moat Farm Junior School

CCTV Policy

Version 1.0

May 2018

A thick green line curves across the top of the page, starting from the left edge, dipping down to form a loop, and then extending towards the right edge.

Contents

1. Introduction	3
2. Objectives of the CCTV Policy	3
3. Statement of Intent	3
4. The Data Protection Principles	4
5. Operational Control & Protocols	4
6. Monitoring Procedure	5
7. Recorded Material Procedures	6
8. Record Keeping / Incident Logs	7
9. Retention of Data	7
10. Breaches of the Policy (including breaches of security)	7
11. Assessment of the CCTV System	8
12. Complaints	8
13. Access by the Data Subject	8
14. Further Information	9

1. Introduction

- 1.1 The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Moat Farm Junior School Trust, hereafter referred to as 'the School'.
 - 1.2 The CCTV system is owned by the school.
- 1.3 The system comprises of 20 cameras 12 Acti ACM 1231, 3 Acti E11, 1 Acti KCN5211-1 and 4 Acti ACN4200-4. Appended to this document is a plan of the building showing the location of all cameras, monitors and the system control centre within the school buildings and on the school site.
- 1.4 On a day to day basis, cameras are monitored by Richard Norton, Site Manager. Recorded images from any camera can only be accessed with express permission from the Head Teacher. The IT staff have access to the system to assist with technical issues only.
- 1.5 The systems will not be used for any other purpose than those set out in this document without prior consultation with the Head Teacher, and where appropriate, notification to staff.
- 1.6 This Policy has been drafted in compliance with the requirements of the General Data Protection Regulation.
- 1.7 The ongoing suitability of the School CCTV Policy will be reviewed annually by the School Governing Body.

2. Objectives of the CCTV Policy

This Policy covers the use of CCTV systems, which capture moving and still images of people who could be identified, for the following purposes;

- To protect School buildings, and their assets within
- To increase personal safety of those within, and visiting the school community
- To act as a deterrent for violent behaviour and damage to the school
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and disciplining offenders

3. Statement of Intent

- 3.1 The School will treat the system and all information, documents and recordings obtained and used as data which are protected by the General Data Protection Regulation, and will be processed in accordance with the requirements of the regulation.
- 3.2 Cameras will be used to monitor activities within the car park, reception and the corridors to identify criminal activity occurring, anticipated or

perceived, and in order to ensure the safety and wellbeing of the School community.

- 3.3 The school will only operate overt surveillance, and will display signs in the areas of the school where this is in operation. Covert surveillance (i.e. which is intentionally not shared with the individuals being recorded) is not condoned by the school.
- 3.4 Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the school CCTV.
- 3.5 The CCTV system will not be trained on individuals unless an immediate response to an incident is required.
- 3.6 The CCTV system will not be trained on private vehicles or property outside the perimeter of the school.

4. The Data Protection Principles

- 4.1 Data collected from CCTV will be processed in accordance with the principles of the General Data Protection Regulation. As such, all data will be:
 - (a) Processed lawfully, fairly and in a transparent manner in relation to individuals
 - (b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
 - (c) Adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed
 - (d) Accurate and where necessary, kept up to date
 - (e) Kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are processed
 - (f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

5. Operational Control & Protocols

- 5.1 Access to the CCTV system, software and data, will be strictly limited to authorised operators and will be password protected.
- 5.2 The system will be managed by Richard Norton, Site Manager in accordance with the principles and objectives expressed in this Policy.
- 5.3 The day-to-day administration of the system will be the responsibility of Richard Norton, Site Manager during the day, out of hours and at weekends.

- 5.4 The CCTV system will be operated continuously 24 hours a day 365 days a year. Footage is recorded for 30 days before it is recorded over.
- 5.5 The Site Manager will check and confirm the efficiency of the system daily and in particular, to confirm that the equipment is properly recording and that cameras are functional.
- 5.6 The ICT Manager will ensure that **all** staff involved with the operation of the CCTV system are properly trained and fully understand their roles and responsibilities in respect of data protection issues e.g.
 - the user's security policy (procedures to have access to recorded images;
 - the user's disclosure policy;
 - rights of individuals in relation to their recorded images.Training records will be maintained accordingly.
- 5.7 Staff, visitors and others entering areas with CCTV viewing monitors will be subject to particular arrangement as outlined below.
- 5.8 Authorised staff must satisfy themselves over the identity of any other visitors and the purpose of their visit. Where any doubt exists, the CCTV monitors must be turned off.
- 5.9 If an emergency arises out of hours, permission must be obtained from The Head Teacher to view or process recorded material.
- 5.10 Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.
- 5.11 Incidents involving the Emergency Services must be notified to the Head Teacher and Sips Education.

6. Monitoring Procedures

- 6.1 Camera surveillance may be maintained at all times.
- 6.2 Pictures will be continuously recorded.
- 6.3 No covert monitoring will be undertaken until the circumstances have been considered by, and written authorisation obtained from the Head Teacher.

7. Recorded Material Procedures

- 7.1 In order to maintain and preserve the integrity of the recorded material used to record events from the CCTV system, and the facility to use them in any future proceedings, the following procedures for their use and retention **must** be strictly adhered to:

- (i) Each item of recorded material must be identified by a unique mark.
- (ii) The system will register the date and time of recorded material insert, including recorded material reference.
- (iii) Any recorded material required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure recorded material store. If recorded material is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the Controller, dated and returned to the evidence material store.
- (iv) If the recorded material is archived the reference must be noted.

7.2 Recorded materials may be viewed by / released to third parties, only in the following prescribed circumstances, and then only to the extent required by law:

- The police, where any images recorded would assist in a specific criminal inquiry;
- Prosecution agencies, such as the Crown Prosecution Service (CPS);
- Relevant legal representatives such as lawyers and barristers;
- Persons whose images have been recorded and retained, and where disclosure is required by virtue of data protection legislation, or the Freedom of Information Act.

7.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register, maintained by the Controller will be made available for this purpose.

7.4 Viewing of recorded materials by the Police must be recorded in writing and in a log book.

7.5 Should recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1(iii). Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the School, and both the recorded material and information contained on it are to be treated in accordance with this document.

7.6 The school retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material this will be produced from the secure recorded material store, complete in its sealed bag.

- 7.7 Requests for access or disclosure will be recorded and the Head Teacher will make the final decision as to whether the recorded images may be released to persons other than the police.

8. Record Keeping / Incident Logs

- 8.1 The School will maintain adequate and comprehensive records relating to the Management of the system and incidents. Model documents from the installers/providers of CCTV system may be utilised for this purpose.

9. Retention of Data

- 9.1 There are no specific guidelines about the length of time data images should be retained. Consequently, the period of retention will be determined locally, will be documented and understood by those operating the system and will be for the minimum period necessary to meet the objectives of the CCTV scheme. A period of 30 days is considered adequate unless determined otherwise (see 10.2 below)
- 9.2 Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.
- 9.3 Measures to permanently delete data should be clearly understood by persons that operate the system.
- 9.4 Systematic checks should be carried out to ensure the deletion regime is strictly followed. This will be undertaken by the Site Manager.

10. Breaches of the Policy (including breaches of security)

Any breach of the Policy by School staff will be initially investigated by the Site Manager and the Head Teacher to determine disciplinary action, if necessary, and to make recommendations on how to remedy the breach. The school will inform our Data Protection Officer in line with Moat Farm Junior School's Data Breach guidelines.

11. Assessment of the CCTV System

An annual assessment will be undertaken by the Site Manager and IT Department to evaluate the effectiveness of the CCTV system. All assessments and work taken will be logged on a CCTV Assessment Form and saved in the GDPR –CCTV folder in date order.

The outcome of the assessment will be reported to a meeting of the School Governors who will determine if the system is achieving the objectives of the scheme, or if the system requires modification.

12. Complaints

Any complaints about the school's CCTV system should firstly be made, in writing, to The Head Teacher. Complaints will be investigated in accordance with section 11 of this document.

13. Access by the Data Subject

- 13.1 The General Data Protection Regulation provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.
- 13.2 Individuals have the right to submit a subject access request in order to gain access to their personal data.
- 13.3 If the individual is not the focus of the footage i.e. they have not been singled out or had their movements tracked then the images are not classed as 'personal data' and the individual is not entitled to the image under the provisions of Subject Access Requests.
- 13.4 In such instances, the school will verify the identity of the individual making the request before any information is supplied.
- 13.5 All requests will be responded to without delay, and at the most within one month.
- 13.6 Requests for access or disclosure will be recorded and the Head Teacher will make a final decision as to whether recorded images may be released to persons other than the police.
- 13.7 Further guidance can be found in the schools procedure for responding to Subject Access Requests.

14. Further Information

Information in respect of data protection issues may be obtained from the Schools Data Protection Officer SIPS Education 0121 296 3000.

The Information Commissioners website www.ico.gov.uk will contain the most up to date information and should be consulted on a regular basis to ensure all elements of this policy continue to reflect current guidance.

Document produced

4th June 2018

Review date

3rd June 2019

Appendix

*Plan showing the location of **all** cameras, monitoring equipment and system control centre within the School*