Fulston Manor School

CCTV Policy

Version Date:	**May 2023**
Review Date:	**May 2024**
Member of Staff Responsible:	**Mr S Bendon** **Assistant Headteacher**

CCTV POLICY

1. INTRODUCTION

1.1 Fulston Manor School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for students, staff and visitors, and to prevent the loss or damage to school property.

1.2 CCTV images will also be used to investigate anything that is prejudicial to the smooth running of the School including incidents of misbehaviour by students.

1.3 The system comprises a number of fixed and dome cameras.

1.4 The system does not have sound recording capability.

1.5 The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team.

1.6 The CCTV is monitored centrally from the school office, by the ICT support team, site staff and members of the school's leadership team. Only staff who have been trained in data protection are granted monitoring permissions.

1.7 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.

1.8 The school's CCTV Scheme is registered with the Information Commissioner under the terms of the General Data Protection Regulations and Data Protection Act. The use of CCTV, and the associated images and any sound recordings is covered by this and other privacy legislation. This policy outlines the school's use of CCTV and how it complies with the Act.

1.9 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the ICT support team in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

2. STATEMENT OF INTENT

2.1 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

https://ico.org.uk

2.2 CCTV warning signs will be clearly and prominently placed at all external entrances to the school.

2.3 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3. SITING THE CAMERAS

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

3.3 CCTV will only be placed in classrooms if there is high value IT equipment in the room that needs monitoring.

3.4 CCTV will be placed in areas within school that have been identified by staff and students as not being easily monitored.

3.5 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. COVERT MONITORING

4.1 The school may in exceptional circumstances set up covert monitoring. It will always follow the Employment Code published by the ICO. Covert monitoring will only be used when:

i) There are genuine suspicions that criminal activity or equivalent malpractice is taking place.
ii) After a privacy impact assessment has been carried out, and that the justification and methods to be used have been documented and fully authorised in writing by a member of the Senior Leadership Team.
iii) Covert CCTV will only be permitted if it is necessary for collecting evidence, for example where being open about recording would be likely to prevent the detection of a crime (or equivalent malpractice).
iv) There are no alternative methods which are less intrusive that could be considered to obtain the necessary information required.
v) It is strictly targeted at obtaining evidence within a set timeframe and should not continue once an investigation is complete.
vi) Clear rules limiting the disclosure of and access to information obtained are in place.
vii) Covert monitoring will not be used in areas where students or staff would genuinely and reasonably expect to be private (for example, toilets or private offices). If there is to be an exception in cases where serious crime is suspected there should be an intention to involve the police
viii) Other information collected while monitoring should be disregarded and, where feasible, deleted unless it reveals information that no reasonable employer could be expected to ignore.

4.2 Access to recordings of evidence obtained by covert monitoring must be strictly controlled and limited to only those having a legitimate need to view the content. The recoding must be retained in a secure place either digitally or in a locked cabinet if images are in hard copy.

4.3 Covert footage or recordings will not be shared unless it is with a relevant authority such as the police, courts, or formal educational body, and only after receipt of a document setting out their legal bases for requiring the information.

5. Storage and Retention of CCTV Images

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely.

5.3 Recorded data will be stored on the Network Video Recorder (NVR) for approximately 7 days if storage space allows.

6. Access to CCTV Images

6.1 Access to recorded images will be restricted to staff authorised to view them and will not be made more widely available, this currently includes:

- The ICT support team
- Site staff
- Heads of house
- Members of the leadership team

6.2 Staff other than those named above who need access to images will need seek approval from the ICT coordinator or Headteacher and then see the ICT support team to view these images.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

7.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The school will respond to requests within 30 calendar days of receiving the written request.

7.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

8. Access to and Disclose of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 Requests should be made in writing to the Headteacher.

8.3 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.

9. COMPLAINTS

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

10. FURTHER INFORMATION

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition (published by the Information Commissioners Office)
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act
- General Data Protection Regulations (GDPR)
- Human Rights Act 1998
- Protection of Freedoms Act 2012

APPENDIX A - CHECKLIST

This CCTV system and the images produced by it are controlled by Fulston Manor School who are responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act).

Fulston Manor School has considered the need for using CCTV and has decided it is required as described in section 1 of this policy. A review of our use of CCTV will be done annually.

	Checked (Date)	**By**	**Date of review**
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	Yes	DFR	01/12/23
There is a named individual who is responsible for the operation of the system.	Yes	DFR	01/12/2023
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	Yes	SBE	01/12/2023
Cameras have been sited so that they provide clear images.	Yes	SBE / DFR	01/12/2023
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Yes	SBE /DFR	01/12/2023
There are visible signs showing that CCTV is in operation.	Yes	SBE/DFR	01/12/2023
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Yes	SBE	01/12/2023

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	Yes	SBE	01/12/2023
Except for law enforcement bodies, images will not be provided to third parties.	Yes	SBE	01/12/2023
The School knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.	Yes	SBE	01/12/2023
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Yes	DFR	01/12/2023

APPENDIX B – 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 will ensure that this requirement is fulfilled.

APPENDIX C – THE 12 GUIDING PRINCIPLES

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need

   The use of the surveillance system is covered by section 1.1

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

   Siting of the cameras is covered in section 3, the policy is reviewed annually

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

   Signage has been displayed on the entrances and exits to each building, the contact person is published in this policy and reviewed annually

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

   Appendix A lists all staff with responsibilities, a log of downloaded videos is to be stored in the "SLT Shared Drive"

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them

   CCTV policy clearly highlights the procedures and rules

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

   Section 5 details the storage of images, the spreadsheet in the "SLT shared drive" details when images should be deleted

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

   Sections 6-8 detail access to the system, images and recordings

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

   Section 1.9 covers the procedures and training needs

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

    The NVR is situated in a secure location, where physical access is restricted, all staff who access the system are trained before usage.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

    The CCTV policy is reviewed annually

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

    Section 8 covers this

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

    The CCTV policy is reviewed annually