JOHN TAYLOR MULTI ACADEMY TRUST

John Taylor Free School
CCTV Procedure

Implementation date:	September 2022
Review Date:	September 2024
Supporting Document:	JTMAT CCTV Statement

Contents

Statement....3
Scope....3
Role and Responsibilities....3
System Description....4
Protocols....4
Security....5
Access – Trust Employees & Law Enforcement Agencies....5
Access – Third Parties....6
Complaints Procedure....6
Monitoring and Review....6
Appendix 1 – CCTV Signage....7
Appendix 2 – CCTV Request Form....8
Appendix 3 – Sample CD/DVD Labelling....9
Appendix 4 – CCTV Checklist....10
Appendix 5 – CCTV Request Workflow (Trust employees and law enforcement agencies)....11

Statement

This procedure seeks to ensure that the Close Circuit Television (CCTV) system used at John Taylor Free School (JTFS) is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018")). It also seeks to ensure compliance with privacy law. It takes into account best practice as set out in codes of practice issued by John Taylor Multi Academy Trust (JTMAT), the Information Commissioner and by the Home Office. JTFS therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 1.2, and only if it is proportionate to that aim.

1.1. JTFS seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property and premises. JTFS therefore deploys CCTV to:

- promote a safe community and to monitor the safety and security of its premises and its assets;
- assist in the safeguarding of staff, students and other third parties on its premises;
- assist in the prevention, investigation and detection of crime and other activities which breach policies and procedures.
- assist in the promotion of safe and appropriate use of the areas of school and school grounds by all stakeholders – students, staff, parents etc.
- assist in the safeguarding of staff, students, other third parties and property whilst on school transport

1.2. This procedure will be reviewed annually by the Head of School to assess compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV system remains justified.

Scope

2.1. This document applies to CCTV systems used by JTFS.

2.2. The procedure does not apply to any webcams, standard (domestic) photographic equipment such as digital/video cameras and mobile devices and classroom recording system as used within the school grounds.

2.3. The procedure does cover cameras that may be deployed at times of the schools choosing for example on the home to school transport in order to support the legitimate aims outlined in clause 1.2

2.4. This procedure applies to all JTFS staff, contractors and agents who operate, or supervise the operation of, the CCTV.

Role and Responsibilities

3.1. Head of School has the overall responsibility for this procedure, but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this document. All relevant members of staff have been made aware of this procedure and the Trust CCTV Statement and have received appropriate training.

3.2. The Senior ICT Technician is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 1.1 of this document. Where new surveillance systems are proposed the school will consult with the Trust's GDPR Lead and Data Protection Officer to determine whether a prior privacy impact assessment is required.

3.3. Only the appointed school's maintenance contractor (Trinity) for CCTV system is authorised to install and/or maintain it.

3.4. The Senior ICT Technician is responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the network software. The list of such locations and the list of persons authorised to view CCTV images is maintained by the Senior ICT Technician.

3.5. Changes in the use of JTFS's CCTV system can be implemented only in consultation with the Trust's GDPR Lead and the Data Protection Officer.

System Description

4.1. The CCTV systems installed in and around JTFS's estate cover building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas. They continuously record activities in these areas and some of the cameras are set to motion detection.

4.2. CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities etc. However areas surrounding these areas e.g. hand washing areas outside of toilets, are covered by CCTV coverage.

4.3. CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors and members of the public are made aware that they are entering an area with CCTV. The signs also contain contact details for the person responsible for CCTV.

4.4. The contact point indicated on the CCTV signs around JTFS should be available to members of the public during normal business hours.

4.6. CCTV cameras are installed in specific locations in pursuit of a legitimate aim, as set out in clause 1.2.

4.7. All CCTV systems are capable of storing recorded images for a specified time, this is known as a data retention period. The overall retention period for the system is 1 month.

Protocols

5.1. The surveillance system will be registered with the ICO by JTMAT in line with data protection legislation.

5.2. The surveillance system is a closed digital system which does not record audio.

5.3. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. An example of the signage used can be found in Appendix 1.

5.4. The CCTV system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

5.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

5.6. The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

Security

6.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

6.2. The school's authorised CCTV system operators are:

- Senior ICT Technician
- ICT Technician
- Site Supervisor
- Caretaker

6.3. The schools authorisers for the CCTV system are:

- Senior Leadership Team members

6.4. The schools authorised viewers are:

- Senior Leadership Team members
- Progress Leaders
- Student Support Team members

6.5. The main control facility is kept secure and locked when not in use.

6.6. Surveillance and CCTV systems will not be intrusive.

6.7. Any cameras that present faults will be repaired as soon as reasonably practical as to avoid any risk of a data breach.

Access – Trust Employees & Law Enforcement Agencies

7.1. Only those named in clause 6.2 can access the CCTV system, and only those named in clause 6.4 can view the system following authorisation.

7.2. Any request must be compatible with the reasons for processing outlined in clause 1.2.

7.3. All viewing and any subsequent disclosure of CCTV images is recorded in the CCTV Request System and contains:

- The name of the requester. If external to the school their address
- The date, time and camera locations viewed
- A reason for viewing or disclosing this information
- Crime number if requested by the police or other law enforcement agency
- Who approved and fulfilled the request
- A record of any copies made.

An example request form can found in Appendix 2.

7.4. Images or footage taken off the system must be transferred to a non-writable media such as CD/DVD or an appropriate shared location to ensure integrity with a minimum of 2 copies one to be retained by the system administrator. An example of the information required can be found in Appendix 3.

7.5. Requests from Trust employees and law enforcement agencies must be made as detailed in clause 7.3. A workflow detailing the stages a request must go through can be found in Appendix 5.

Access – Third Parties

8.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

8.2. Individuals have the right to submit a Subject Access Request. Each request will be accessed individually in line with the Trust's SAR Procedure to ensure the rights and freedoms of all identifiable (directly or indirectly) individuals are protected.

8.2. Requests for CCTV information under the Freedom of Information Act will be considered in accordance with that regime.

Complaints Procedure

9.1 Any complaints relating to the CCTV system will be dealt with as per the Compliments, Comments and Complaints Policy available on the Trust and/or school's website.

9.2 Complaints in relation to the release of images should be addressed to the Trust's Data Protection Officer.

Monitoring and Review

10.1. JTFS undertakes regular reviews of the CCTV system to ensure its use continues to be justified.

10.2. During each review a checklist which can be found in Appendix 4 is completed.

Appendix 1 – CCTV Signage

24 hour CCTV in operation

Your safety is important, closed-circuit television system is operated on these premises for the purpose of prevention and detection of crime, safety and good management.

This scheme is controlled by:

For further information contact:

Appendix 2 – CCTV Request Form

JTFS will hold an electronic copy of this form centrally which will include all of the information below. The below is a paper copy of the same information and will be used as a back-up if the electronic file is unavailable.

JTFS CCTV Request Form

Requester Name		Date of Request	
Location of Incident to be Reviewed			
Time of Incident to Be Reviewed			
Reason for Request			
Approver Name		Approver Signature	
		Date / Time	

Address of Requester if external to JTMAT	

To be completed by the Operator

Which Cameras Observed	
Copies Made? (Yes / No)	
If Yes – Reference Number	
Police Crime Number if relevant	

Appendix 3 – Sample CD/DVD Labelling

Appendix 4 – CCTV Checklist

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has 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.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
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.			
Except for law enforcement bodies, images will not be provided to third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation 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.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix 5 – CCTV Request Workflow (Trust employees and law enforcement agencies)