JOHN TAYLOR MULTI ACADEMY TRUST

CCTV Policy

Implementation date: March 2018

Review date: March 2019

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	10/04/2017	First Draft.
2.0	M. Crompton	10/11/2017	Major changes to reflect new legislation (GDPR) and best practice advice.
2.1	M. Crompton	09/03/2018	Changes as per the Audit Committee comments

Context

The UK is recognised as a leading user of CCTV and the public are used to seeing CCTV cameras on virtually every high street. Such systems continue to enjoy general public support but they do involve intrusion into the lives of ordinary people as they go about their day to day business and can raise wider privacy concerns.

We know the public expect CCTV to be used responsibly with proper safeguards in place. We have developed this CCTV policy to comply with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) to inspire confidence that we are using CCTV responsibly.

Images of people are covered by the Data Protection Act and General Data Protection Regulation (GDPR) and so is information about people which is derived from images – for example, vehicle registration numbers.

Further Reading

- CCTV – ICO Code of Practice https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- Data Protection Act (DPA) https://ico.org.uk/for-organisations/guide-to-data-protection/
- General Data Protection Regulation (GDPR) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
- Security Services (External Contractor) https://www.securitywiseservices.com/
- Lockdown Policy & Procedure

Introduction

John Taylor Multi Academy Trust (JTMAT) is fully committed to the safety of its staff, students and visitors and to this extent has invested in the security of its buildings and facilities. The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system within the Trust.

Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the Data Protection Act, General Data Protection Regulation (GDPR) and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that Act. The use of CCTV by schools is covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.

All cameras maybe monitored and are only available for use by approved members of staff. The CCTV system is owned by the Trust and will be subject to a review annually.

Persons Responsible

Each Head of School/Headteacher herein named the Systems Administrator at each academy is responsible for the implementation and enforcement of this policy within their respective academies.
The above system administrator has named the following individuals responsible for the day to day management of the CCTV systems implemented at each academy:

- Site Manager
- Strategic Network Manager
- Business Manager
- Deputy Headteacher

User of the System

The Systems Administrator has the authority to grant access to specific individuals to view and access recordings. Each individual will be given a separate account for accessing the system when that feature is available.

User Responsibilities

All users of the CCTV system have the following responsibilities:

- To uphold the arrangements of this policy.
- To handle images/data securely and responsibly, within the aims of the policy. Staff need to be aware that they could be committing a criminal offence if they misuse CCTV images. To uphold the recorded procedure for subject access requests.
- To report any breach of this policy or procedure to the System Manager. To attend training / refresher sessions as required

Objectives of the CCTV System

The Trust uses CCTV equipment to provide a safer, more secure environment for students and staff and to prevent bullying, vandalism and theft. Essentially the system is used for:

- To protect the Trust's buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.
- To support the police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- Safeguarding public, student and staff safety.
- Monitoring behaviour; if there is cause for concern and the incident has been reported to an appropriate member of staff.
- To assist in the usage and management of Trust buildings on a day to day basis.

The academy does not use the CCTV system for covert monitoring.

The John Taylor Free School (Branston Locks) in addition to the above will use CCTV equipment for the purposes of staff development training. All staff taking up positions at the aforementioned free school are aware of this prior to appointment.

Location

Cameras are located in those areas where each academy has identified a need and where other solutions are ineffective. The Academies' CCTV system is solely used for the purposes identified above and is not used to monitor staff conduct within lessons unless a serious concern is raised. Cameras will only be used be used in exceptional circumstances in areas where the subject has a heightened expectation of privacy e.g. changing rooms and toilets. In these areas, the Trust will use increased signage in order that those under surveillance are fully aware of its use.

Identification

In areas where CCTV is used the Trust will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

The signs will be:

- Clearly visible
- Contain details of the organisation operating the scheme, the purpose for using CCTV and who to contact about the scheme.

Image storage and retention

Recorded images and sound will be stored in a way that ensures its integrity and in a way that allows specific times and dates to be identified. Access to live images is restricted to a list of approved users unless the monitor displays a scene which is in plain sight from the monitored location. Recorded images can only be viewed in a restricted area by approved staff. The recorded images are viewed only when there is a clear reason for this to happen.

The Trust reserves the right to use images captured on CCTV where there is activity that the Trust cannot be expected to ignore such as criminal activity, safeguarding, potential gross misconduct, or behaviour which puts others at risk. Images retained for evidential purposes will be retained in a locked area accessible by the system administrator only. Where images are retained, the system administrator will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed.

Neither the Data Protection Act nor the Information and Records Management Society prescribe any specific minimum or maximum periods which apply to CCTV recorded images. CCTV images are retained for a period of between 7-31 days depending on the location of the camera and its individual context. For example, cameras within with Trust building may only be stored for 7 days as incidents will come to light quickly.

Disclosure

Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

Academy Members

Disclosure of the recorded images or sound to member of the Trust community can only be authorised by the system administrator or those with delegated access. Disclosure will only be granted:

- If its release is fair to the individuals concerned.
- If there is an overriding legal obligation (e.g. information access rights).
- If it is consistent with the purpose for which the system was established.

Third Parties

Disclosure of the recorded images to third parties can only be authorised by the system administrator. Disclosure will only be granted:

- If its release is fair to the individuals concerned.
- If there is an overriding legal obligation (e.g. information access rights).
- If it is consistent with the purpose for which the system was established.

The Request Procedure

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented.

Initial request for disclosure

<table>
<tr><td colspan="3">Initial request for disclosure completed:
https://forms.office.com/Pages/ResponsePage.aspx?id=o9n4cUczDUCoUtIXzz1lTsU_sJeowGlEjhtnaGhhCb9UN1FJTkhTTDhVVkhHSkJVWU81U0g3VkJFUC4u</td></tr>
<tr><td colspan="2">Systems Administrator or nominated person(s) accepts request</td><td>System administrator declines request</td></tr>
<tr><td colspan="2">Disclosure recording sheet completed</td><td>Disclosure recording sheet completed detailing the reason why the request was declined</td></tr>
<tr><td>Internal Request</td><td>Third Party Request</td><td rowspan="6"></td></tr>
<tr><td colspan="2">Disclosure processed by the person responsible for day-to-day management</td></tr>
<tr><td>The above is usually done in the presence of the person requesting the disclosure</td><td>Images/sound downloaded and copied to 2 CD/DVDs. Detailing the following: Date, Time, Request number</td></tr>
<tr><td rowspan="2">If a copy is required follow the procedure described for third parties</td><td>One copied it retained by the academy and stored securely</td></tr>
<tr><td>One copied sealed and signed for by the person requesting the disclosure</td></tr>
<tr><td colspan="2">Disclosure recording sheet updated</td></tr>
</table>

Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom “personal data” relate) with a right to data held about themselves, including those obtained by CCTV. Request for Data Subject Access should be made I writing to the Head of School/Headteacher.

System Maintenance and Monitoring

The Trust undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

- Completed Code of Practice Checklist
- Its stated purpose
- The location of cameras
- The images recorded and the length of time they may be stored for CCTV policy and procedure

The CCTV systems are owned by the Trust and jointly operated by the Trust and in some instances an off-site monitoring firm.

Complaints

Any complaints about the academies' CCTV system should follow the relevant academies' complaints procedure.

Appendix 1 Code of Practice Check List

This CCTV system and the images produced by it are controlled by the academy who is 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 1998)

The Trust has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of our community. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	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 (eg 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 2 Disclosure Request

Sample Disclosure Request

–

CCTV

Playback Request Form

Name: _____ **Location of area to view:** _____

Address: _____ **Date & Time of incident:** _____

City: _____ **Requesting viewing on:** _____

County: _____ **Post code:** _____

Tel. Number: _____

Mobile Number: _____

Reason for request: _____

Signed: _____ **Date:** _____

---------- ***Please submit this document to the system administrator*** ----------

Date Received: _____

Ref No: _____

Approved: **Yes/No**

Reason: _____

Signed: **Date:** _____

---------- ***Please submit this document to the day to day manager*** ----------

Date Received: _____

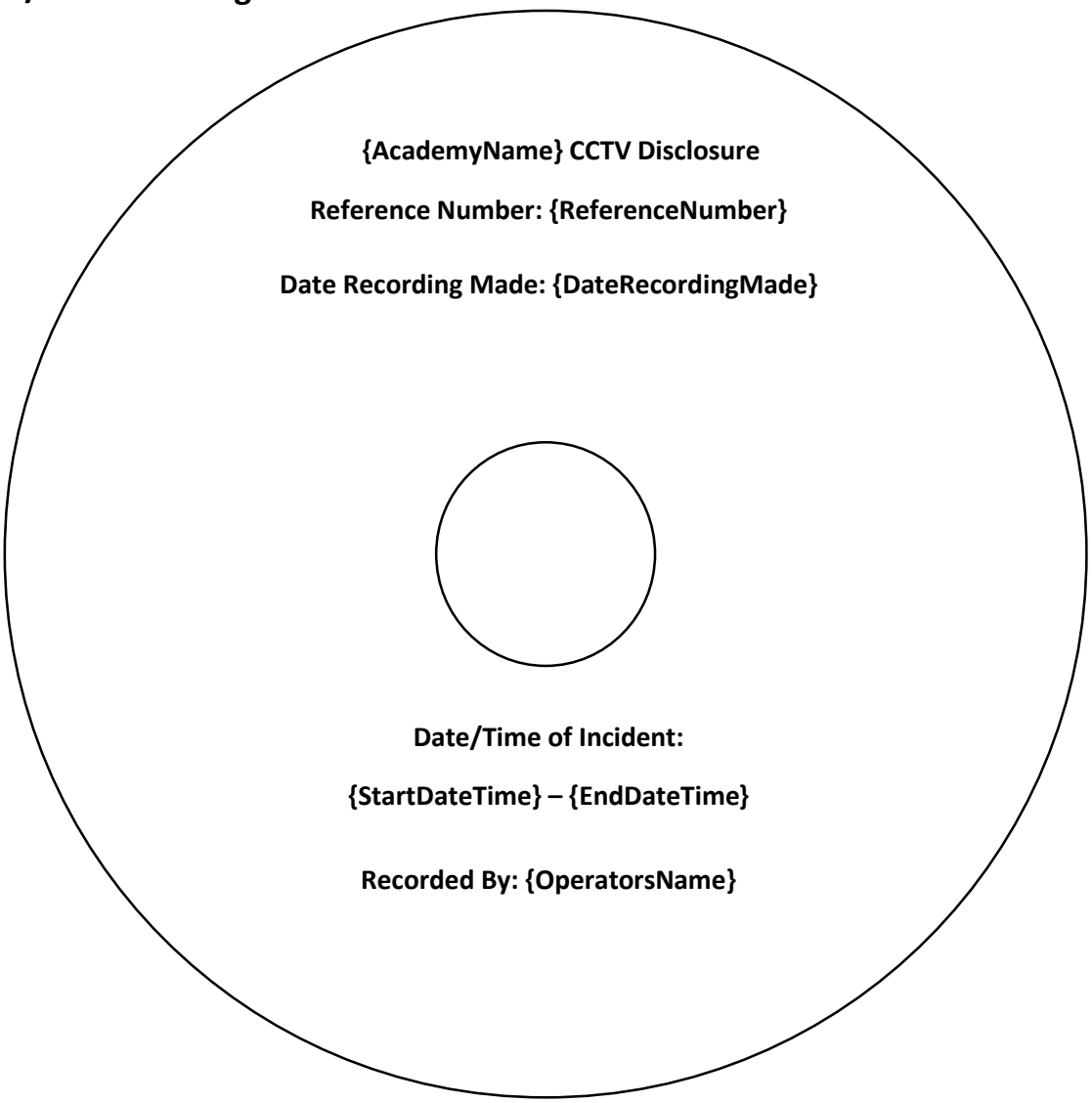
Date disclosure took place: _____

Requestor present: **Yes/No**

Copy Made: **Yes/No** *Ensure 2 copies are made and one returned with tis form to the system administrator

Signed: _____ **Date:** _____

Sample CD/DVD Labelling



Appendix 3 Sample CCTV Sign

WARNING!

CCTV

IN OPERATION

Operated By:

John Taylor Multi-Academy Trust

For further information contact:

-

Head of School