Thomas Bullock CE Primary Academy

CCTV Policy

September 2021

POLICY FOR THE USE OF C.C.T.V. SYSTEMS AT Thomas Bullock CE Primary Academy

This policy is issued by Thomas Bullock CE Primary Academy.

1. **Definitions**
   "The School" – Thomas Bullock CE Primary Academy.
   "Data Controller" - The schools Data Controller is the Headteacher
   "CCTV Operator" Employees of the school with the knowledge and permission to operate the CCTV and retrieve footage.

2. **Introduction**
   The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at the school.
   The system comprises a number of static cameras located throughout the school site
   All cameras covering communal areas can be monitored from the Leadership Office only.

This policy is based upon the Code of Practice published by the Information Commissioner, which set out the standards for the requirements of the Data Protection Act 2018(DPA) and General Data Protection Regulation (GDPR) to be met. It should also be read in conjunction with the Trust Data Protection Policy and Data Retention Policy.

The CCTV system and Data are owned by the academy.

3. **Objectives of the school CCTV system are** :
   To increase personal safety and reduce the fear of crime.
   To support the Police in a bid to deter and detect crime.
   To protect the school buildings and assets of the school.
   To assist in managing the school.

4. **Statement of Intent**
   The CCTV system is registered with the Information Commissioner under the terms of the DPA and GDPR and seeks to comply with the requirements of the Commissioners Code of Practice.

   The school will treat the system and all information, documents and recordings obtained and used, as Data, which are protected by the GDPR.

   The system installed is compliant with the DPA, GDPR, Human Rights Act (art.8) and the Regulation of Investigatory Powers Act (RIPA)

   Cameras will be used to monitor activities within the school and its surrounding grounds to identify criminal activity actually occurring, anticipated or perceived and for the purpose of securing and developing the safety and wellbeing of the school and its staff, students and visitors.

   Materials of knowledge secured as a result of CCTV will not be used for any commercial purpose. Information transferred to any digital media will only be used for the investigation of a specific crime or incident.

Release to any third party would only be allowed with the written authority of the Police if this was required by them as part of a Police investigation.
Nothing above will restrict an individuals right to Subject Data Access.

5. **Subject Data Access**
   In accordance with Section 7 of the DPA as amended by the GDPR an individual who believes that their image has been captured by this scheme is entitled to make a request to the Data Controller. There is no fee. Upon supply of essential information, a system search will be conducted and the individual will be allowed to access the personal data held.
   The statutory time limit to provide the data is 1 month.
   All subject access requests should be referred in the first instance to the Data Controller.
   All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and how such requests are to be dealt with.
   The attached form should be completed **by staff** ensuring that all the necessary information has been obtained to enable a detailed search.

   Prior to any authorised disclosure, the Data Controller will need to determine whether the images of another 'third party' individual features in the personal data being applied for and whether these 'third party' images are held under a duty of confidence. If the 'third party' images are not to be disclosed the System Manager shall arrange for the 'third party' images to be disguised or blurred at a cost to the subject data access requestor.

   If the Data Controller decides that a subject access request from an individual is not to be complied with, the following should be documented:
   The identity of the individual making the request.
   The date of the request.
   The reason(s) for refusing to supply the images requested.
   The name and signature of the person making the decision.

6. **GDPR right to erasure**
   GDPR provides subjects with the new 'right to erasure'.
   CCTV footage within the school is only retained for no more than 30 days before being automatically erased. Therefore rights of erasure will not apply as it is an automated element of our data protection.

Use of Cameras for managing behaviour or CPD

Currently at Thomas Bullock we only use CCTV for external purposes. The use of cameras within classrooms for recording purposes remain under the direct control of the class teacher. The system is so designed as to not be operational in the classrooms until such a time as the teacher initiates the system or the Headteacher from the system control panel. The teacher's laptop is the only part of the system able to jointly record audio and video. The control panel captures only video and has no audio connection.

Constant monitoring by video camera does not make it a proportionate use of personal data therefore teachers should not have cameras set to continuous record.

This policy does not allow teachers to record and retain images of all lessons 'on the off-chance' that to do so might be useful.

When using the system for continuing professional development purposes, the need to do so should be defined and noted on the relevant recording form and in the teachers forward planning.

The Headteacher reserves the right to observe any class at any time from the system control panel, however the Headteacher has no right to record such CCTV footage. Acceptable reasons for the Headteacher to observe a lesson remotely would be: the teacher is an NQT, a new lesson is being taught, a problematic class, a lesson that is likely to provide examples of good practice.

Where appropriate the Headteacher should inform the teacher in advance that observations may be undertaken using the system. If this is not appropriate the teacher should be informed as soon as practicable after the event and the reasons for the observation given. It is deemed as sufficient notice to inform all staff that on a certain day video monitoring may be undertaken.

Addressing Problem Behaviour and Low Level Disruption in Classrooms

To avoid difficulties arising when video footage captured for one purpose is used for another it is important for schools to ensure that any processing is proportionate to the problem that needs addressing. Using footage to find out who in the class has hidden something or was talking behind the teacher's back could be considered disproportionate. Investigating a serious assault would be less problematic. Decisions on whether to use video footage will need to be taken at school management level on a case by case basis.

Constant filming and sound recording is likely to be unacceptable unless there is a pressing need - for example, if there is an ongoing problem of assaults or criminal damage.
The ICO agree that one person's prank is another person's distressing incident but constant video monitoring of all children in a class cannot be justified in their view with reference to the need to address classroom disruption.

Video footage collected for the purpose of CPD cannot be used for the subsequent investigation of trivial behavioural incidents.

Sound Recording

The ICO Code of Practice makes it clear that any classroom based CCTV system must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified.
Clearly, if the system is installed and being used for the purpose of continuing professional development, there is a need to record sound as well as images. In these cases, all those whose images and conversations could be captured should be made aware that this is the case. In addition, the second data protection principle requires that personal data collected for one purpose cannot be further processed for another,

Processing the Images

Standards

1. Images should not be retained for longer than is necessary and unless required for specific investigation or evidential purposes, deleted after 30 days have passed.
2. Once the retention period has expired, the images should be removed or erased.
3. Images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.
4. Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed or be capable of being viewed by anyone other than authorised persons.
5. Access to the recorded images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access.
6. Viewing of the recorded images should take place in a restricted area, for example, in a manager's or designated member of staff's office, Other employees should not be allowed to have access to that area when a viewing is taking place.
7. Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows: (Appendix A)

a. The date and time of removal;
b. The name of the person removing the images;
c. The name(s) of the person(s) viewing the images;
d. The reason for the viewing;
e. The outcome, if any, of the viewing;
f. The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.

8. All operators and employees with access to images should be aware of the procedure that needs to be followed when accessing the recorded images.
9. All operators should be trained in their responsibilities under the Code of Practice, i.e. they should be aware of:

a. The user's security policy e.g. procedures to have access to recorded images;
b. The user's disclosure policy

Access to and disclosure of images to third parties

Standards

All employees should be aware of the restrictions set out in this policy in relation to access to, and disclosure of, recorded images.

1. Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment.
2. All access to the medium on which the images are recorded should be documented.
3. Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, in disclosure will be limited to the following classes of persons/agencies.

- *Law enforcement agencies, where the images recorded would assist in a specific enquiry;*
- *Highways authorities in respect of traffic management matters;*
- *Law enforcement agencies where the images would assist a specific criminal enquiry;*
- *Prosecution Agencies;*

- *Relevant legal representatives*

4. All requests for access or for disclosure should be recorded, if access or disclosure is denied, the reason should be documented,
5. If access to or disclosure of the images is allowed, then the following will be documented. (Appendix B)

- *The date and time at which access was allowed or the date on which disclosure was made;*
- *The identification of any third party who was allowed access or to whom disclosure was made;*
- *The reason for allowing access or disclosure;*
- *Location of the images*
- *Any crime incident number to which images may be relevant*
- *Signature of person authorised to collect the medium – where appropriate.*

6. Recorded images will not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet.
7. If it is intended that images will be made more widely available, that decision should be made by the Headteacher or designated member of staff and the reason for that decision should be documented.
8. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.
9. Any refusal for access or disclosure must be referred in writing to the Trust Data Protection Officer Sharon Money sharon.money@donesc.org

Should any images be required by the Police, we will follow this protocol:

1. The request must be in written form, specifying the date and time (as far as possible) of the image.
2. The rank of the requesting officer must be Inspector or above
3. The school must provide a response to a request within 20 days
4. If the decision is taken not to release the images, then the image in question must be held and not destroyed until all legal avenues have been exhausted.

During times of school closure, the CCTV system will continue to operate as normal.

APPENDIX A

C.C.T.V. Thomas Bullock CE Primary Academy

RECORDING OF VIEWING BY AUTHORISED SCHOOL STAFF

Date and Time Image Viewed:

Date: _____ Time:_____

Name of Persons Viewing the Image:

Name: _____ Designation: _____

Reason for the viewing:

Outcome, if any, of the viewing:

Signed: _____ Headteacher

APPENDIX B

C.C.T.V. – Thomas Bullock CE Primary Academy

RECORDING OF VIEWING BY THIRD PARTY (e.g. Police)

Date and Time Access Allowed:

Date: _____ Time: _____

Identification of any third party who was allowed access:

Names of school staff present:

Reason for allowing access:

Crime incident number if applicable:

Location of the images:

Signature of the person authorised to collect the medium – where appropriate:

Date and time copy created for evidential purposes:

Date: _____ Time:_____

DVD Record Number: _____

APPENDIX C

C.C.T.V. – Thomas Bullock CE Primary Academy

FORM TO REQUEST ACCESS TO CCTV IMAGES

NAME:

ADDRESS:

DATE OF BIRTH:

TELEPHONE NUMBER:

Date image recorded:

Time image recorded:

Location:

Advice sought from Trust DPO Yes/No