CCTV Policy

Tees Valley Education Trust

Version:	1.0	
Ratified by:	Trust Board	Chairs signature:
Date ratified:		
Name of originator/author:	A Porter	
Circulated to:	All Dormanstown Staff	
Date issued:		
Review date:		
Target audience:	ALL TRUST STAFF MEMBERS/VISITORS/PARENTS	

1 INTRODUCTION

Dormanstown Primary Academy uses closed circuit television (CCTV) images to monitor the site buildings & security and for the safeguarding of children in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to the property.

The system comprises a number of fixed and dome cameras; it does have sound recording capabilities, however this is fully disabled.

The CCTV system is owned and operated by the academy, the deployment of which is determined by the academies leadership team.

The CCTV system is accessed by designated staff. They are the Executive Principal, Head of Academy, Deputy Heads of Academy and the Operations & Communications Manager. Staff accessing the system must adopt the Surveillance Camera Code of Practice when using the system (Appendix 3).

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

The academies CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated image recordings are covered by the Data Protection Act 1998. This policy outlines the academies use of CCTV and how it complies with the Act.

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained by the trusts data controller 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

The academy 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/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

CCTV warning signs are clearly and prominently placed at all external entrances to the academy. Signs contain details of the purpose for using CCTV (see appendix B). In areas where CCTV is used, the academy will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

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 OF CAMERAS

Cameras are sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated. The Pelco dome cameras have further privacy features enabled to block out houses close to the academy site. The academy will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

The academy will make every effort to position cameras so that their coverage is restricted to the academy premises, which includes outdoor areas.

CCTV will not be used in classroom areas. CCTV cameras are located in group/circulation spaces where supervision is not always possible. 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 STORAGE AND RETENTION OF CCTV IMAGES

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.

Recordings will normally be stored for 21 days on the system, after which they will be automatically deleted unless retention beyond this data is required as part of an on-going investigation. All retained data will be stored securely.

The system is maintained by a third party organisation to ensure the integrity of the system and its recordings.

5 ACCESS TO CCTV IMAGES

Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

6 SUBJECT ACCESS REQUESTS (SAR)

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

All requests should be made in writing to the Head of Academy. 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.

In instances where footage includes images of other individuals, it is highly likely that a request will be declined. The academy 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.

The Academy will respond to requests within 10 calendar days of receiving the written request and fee.

A fee of up to £10 will be charged per request.

7 ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

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 academy where these would reasonably need access to the data (e.g. investigators).

Requests should be made in writing to the Executive Principal/Head of Academy.

The data may be used within the academies discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

8 COMPLAINTS

Complaints and enquiries about the operation of CCTV within the academy should be directed to the Executive Principal/Head of Academy in the first instance.

9 FURTHER INFORMATION

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

CCTV Code of Practice (published by the Information Commissioners Office)

www.ico.gov.uk

Regulation of Investigatory Powers Act (RIPA) 2000

Data Protection Act 1998

Appendix 1 - Checklist

This CCTV system and the images produced by it are controlled by the Operations & Communications Manager 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). We conduct a bi-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.	Yes	Adam Porter	31/10/2016
There is a named individual who is responsible for the operation of the system.	Yes	Adam Porter	
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.	Yes		
Cameras have been sited so that they provide clear images.	Yes		
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Yes		
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).	Yes		
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Yes		
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		
Except for law enforcement bodies, images will not be provided to third parties.	Yes		
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	Yes		
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.	Yes		
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Yes		

Appendix 2

CCTV Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The school is to ensure that this requirement is fulfilled.

The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The contact telephone number or address for enquiries

Appendix 3

The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

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

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.

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

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.

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.

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.

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.

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

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.

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.

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.