



# CCTV Policy December 2019

*Office use*

<b>Published:</b> December 2019	<b>Next review:</b> January 2022	<b>Statutory/non:</b> Statutory	<b>Lead:</b> Andrew Wilson, Head of Estates and Facilities Management
<b>Associated documents:</b>			
<ul style="list-style-type: none"> <li>In the picture: A data protection code of practice for surveillance cameras and personal information. ICO June 2017</li> <li>Data Protection Act 1998</li> </ul>		<ul style="list-style-type: none"> <li>General Data Protection Regulations (GDPR) May 2018</li> </ul>	
<b>Links to:</b>			
<a href="https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf">//ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf</a>			

## Contents

1	Statement of intent.....	3
2	Operation of the systems .....	3
3	Protocols.....	4
4	Complaints.....	4
5	Access by the Data Subject .....	5
6	Public information .....	5

## **1 Statement of intent**

The use of Closed Circuit Television (CCTV) within our academy sites is to ensure that;

- Students, staff and members of the public using these facilities are safeguarded
- The facilities are secure
- It deters anti-social or illegal activity
- We have the ability to aid the police to identify persons if an offence is committed

Whilst undertaking this our CCTV systems are registered with the Information Commissioners Office under the terms of the General Data Protection Regulations (GDPR)

The purpose of this policy is to manage and regulate the use of these CCTV systems, how they are operated, who can view the images and the associated stored data.

## **2 Operation of the systems**

### **Trust managed academies**

The overall approach to the systems will be administered centrally by the Diverse Academies Trust and National Church of England Academy Trust and will be installed and managed in accordance with the principles and objectives expressed in the ICO Code of Practice and registered with the ICO as Data Controllers.

The day-to-day management of each system will be the responsibility of the Academies Principals, their deputy, Academy Business Managers or other nominated senior member of staff and the Site Managers.

The CCTV systems will be operated 24 hours each day, all year round.

### **PFI academies**

Some of our academies are Private Finance Initiatives (PFI), where we operate the academic programme, the sites and facilities are managed by an outsourced FM provider.

In these situations, the FM providers are responsible for the administration and management of the CCTV systems in accordance with their own policies, all statutory obligations and codes of practice.

As such we work with the FM provider and are bound to follow their policies.

A member of the Senior Leadership Team at each site that can request access to view information/images in the event of an incident or situation occurring.

### **3 Protocols**

- The CCTV systems are closed digital system.
- Warning signs have been placed throughout the premises where the CCTV system is active.
- The CCTV system has been designed for maximum effectiveness and efficiency. The academy cannot however guarantee that every incident will be detected or covered and 'blind spots' may exist.
- The CCTV system will not be trained on individuals unless an immediate response to an incident is required.
- The CCTV system will not be trained on private vehicles or property outside the perimeter of the school.
- Access to the system will be strictly limited to those staff already noted.
- Images/recorded data can only be viewed with authorised consent of those staff noted and recorded within the CCTV register.
- All stored data will be kept in a secure locked area or via password protected access to a secure server.
- Recordings will only be released following submission of a completed request form on the authority of the Principal (or Facilities Management provider for PFI sites), then only to the Police or as required under a Subject Access Request.
- Sites may use visual display screens, these are generally within reception or similar areas to ensure access to the site and main doors are monitored during operational hours. These screens should not be visible to students or members of the public.
- Images will only be retained for as long as they are required. The system will automatically delete recordings after 31 days.
- Be used only for the purposes for which it is intended, including supporting public safety, protection of students, staff and law enforcement.

### **4 Complaints**

Any complaints about the CCTV systems should be addressed to the Principal or a senior member of staff of the appropriate academy in the first instance. If they you wish to pursue this matter further refer to the Trust Complaints Policy available on the Academy or main Trust website.

Complaints will be investigated in accordance with this policy.

## **5 Access by the Data Subject**

The General Data Protection Regulation provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access should be made to the Principal of the appropriate academy.

## **6 Public information**

A copy of this policy is available to the public on the trust website.