



# **CCTV Policy**

<b>Document control table</b>			
<b>Document title:</b>	CCTV Policy		
<b>Author (name &amp; job title):</b>	Stuart Jones, Director of Technology		
<b>Version number:</b>	V2		
<b>Policy Status</b>	For Approval		
<b>Date approved:</b>	April 2018		
<b>Approved by:</b>	OGAT Board		
<b>Date of review:</b>	April 2019		
<b>Document History</b>			
<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Note of revisions</b>
V1	26/1/18	Stuart Jones	First release
V2	20/3/18	Stuart Jones	Clarifications and amendments to delegation and access information.

## **CCTV Policy**

### **Table of Contents**

1.	Introduction	page 4
2.	Purpose and Types of CCTV	page 4
3.	Responsible Persons	page 4
4.	Covert Recording	page 4
5.	Signage	page 5
6.	Fixed Installation CCTV	page 5
7.	Vehicle CCTV	page 7
8.	Accessing Recorded Images	page 8
9.	Training	Page 9

## **1. Introduction**

Outwood Grange Academies Trust owns and operates Closed Circuit Television (CCTV) within its academies in order to provide a safe and secure environment for students, staff and visitors, as well as to protect academy property.

This document sets out the accepted use and management of the CCTV equipment and images in order to ensure academies comply with appropriate legislation. It has been produced in line with the Information Commissioner's CCTV Code of Practice.

## **2. Purpose and Types of CCTV**

Outwood Grange Academies Trust owns and operates CCTV systems for the purpose of:

- Providing a safe and secure environment for students, staff and visitors
- Maintaining the security of sites, buildings and associated contents

The use of CCTV for any other purpose may be unlawful and may bring the system into disrepute.

Outwood Grange Academies Trust has approved the following types of CCTV for potential use:

- Fixed Installation (buildings and premises)
- Vehicle

Wireless cameras are not approved for use at this time.

## **3. Responsible Persons**

Within each academy, primary responsibility for CCTV will lay with the Principal and Business Manager. The Business Manager may delegate the day to day duties of CCTV operation to a Facilities/Premises Manager or similar role where appropriate.

## **4. Covert Recording**

Covert surveillance is that which is carried out in a manner calculated to ensure that subjects of it are unaware it is, or may be taking place. No such recording will be carried out by any academy.

Any use of CCTV systems or materials in this manner may result in disciplinary action for cases considered misconduct / gross misconduct.

## **5. Signage**

In accordance with the Information Commissioner's CCTV code of practice, appropriate signs must be displayed where CCTV is operating.

All Outwood Grange Academies Trust buildings/premises and vehicles fitted with CCTV systems will prominently display public awareness signs detailing:

- The academy responsible for the CCTV scheme (unless it is otherwise obvious)
- That CCTV equipment is in operation
- Purpose of the CCTV system
- Academy contact telephone number

## **6. Fixed Installation CCTV**

### **6.1 Siting of Fixed Installation CCTV**

Fixed installation CCTV cameras should be professionally installed and appropriately specified to meet the requirements of this policy. To ensure quality and reliability, cabling should also be professionally installed and terminated with test certificates where appropriate.

If the camera is expected to operate over the computer network, The Network Manager is to be consulted on the full installation to ensure provisions are sufficient to support the device.

### **6.2 Documentation**

Documentation detailing the location of fixed CCTV cameras and their coverage area should be kept by the academy and be up to date.

Where the camera information such as a location or date and time stamp is recorded along with the image, this information must be accurate.

### **6.3 Operators**

CCTV images can sometimes be of a sensitive nature, and therefore access should be tightly controlled and only granted to specific staff for appropriate reasons.

- Business Manager – The academy Business Manager is responsible for CCTV and should have full access to view all cameras along with all live and recorded footage.

- Premises Manager/Facilities Manager/Site Manager – It is likely that in most cases, the Business Manager will delegate the day to day CCTV operations to this role and therefore full access to all cameras and live/recorded footage will be required.
- Premises Team – The premises team should have access to live footage from all cameras. Access to recorded footage should be restricted.
- Network Manager/Assistant Network Manager – Where CCTV equipment connects in some way to the academy computer network, the Network Manager and Assistant Network Manager should have full access to the configuration of the CCTV systems as well as live and recorded footage of all cameras to ensure proper operation of equipment.
- ICT Support Technicians – Should have access to live camera feeds to aid troubleshooting and ensure equipment is operating properly. ICT Technicians must not have access to recorded footage.

Additional access can be delegated by the Business Manager to an individual or individuals (including those in roles listed above) following consultation with their line manager. Consideration should be given and documented as to the appropriateness of any access, the location in which the footage would be viewed and the risk of inappropriate use. Training in handling CCTV images should be provided before any access is given. Delegation outside of the positions defined above is considered to be to the person and not the role, therefore the agreement of both parties is required.

#### **6.4 Maintenance**

The overall maintenance of the system will be the responsibility of the Business Manager. All CCTV systems should have a valid maintenance contract with an appropriate supplier and recorded on the Every system.

The Business Manager or Premises/Facilities Manager should be informed of any malfunction so it can be investigated and reported to the maintenance contractor.

## **7. Vehicle CCTV**

Vehicle CCTV refers to the process of recording footage within the passenger area of an academy minibus for the safety of students and staff. It may also refer to the process of recording the view from the front or rear of the vehicle for safety and insurance purposes.

### **7.1 Siting of Vehicle CCTV**

Vehicle mounted CCTV should be hardwired and professionally installed to record whilst the engine is running.

### **7.2 Documentation**

Documentation regarding the installation of the vehicle CCTV should be kept in the vehicle file.

Where camera information such as location, speed, or date and time is recorded with the image, this information must be accurate and verified termly.

### **7.3 Operators**

Only the Business Manager and Facilities/Premises/Site Manager should have access to view and retrieve the footage from vehicle CCTV.

### **7.4 Maintenance**

The overall maintenance of the system will be the responsibility of the Business Manager. All CCTV systems should have a valid maintenance contract with an appropriate supplier and be recorded on the Every system.

The Business Manager or Premises/Facilities Manager should be informed of any malfunction so it can be investigated and reported to the maintenance contractor.

## 8. Accessing Recorded Images

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established.

Access to, and disclosure of, images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are retained, and also ensure that the images can be used as evidence if required. Images can only be disclosed in accordance with the purposes for which they were originally collected.

**Access to recorded images by parties not defined elsewhere in this policy will only be given after the appropriate authorisation from the Business Manager.**

Under the Data Protection Act 1998 individuals have a right to view any recorded images of themselves and, unless they agree otherwise, to be provided with a copy of the images. The applicant must make their subject access request in writing.

When an applicant makes a subject access request for CCTV or other video images it is necessary for them to provide:

- Proof of their identity.
- A clear description of the location in which they believe they were recorded on CCTV, along with the date and time.
- A clear picture of themselves, to aid identification and enable a comparison with CCTV footage.
- Ideally a description of what they were wearing at the time the images were captured.

A subject access request will be dealt with within the required response time of 40 calendar days, subject to any extensions as stated within the Data Protection Act.

If images of third parties are also shown with the images of the applicant, consideration must be given to whether providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress. If this would be the case then the footage cannot be released unless it is possible to obscure those third parties.

Disclosure of the recorded images unedited or edited may be made where the images are required for:

- The prevention and detection of crime.
- The apprehension or prosecution of offenders.
- Where disclosure is required by law including an order of a court.
- Disclosure is made in connection with legal proceedings.



## **Training**

Appropriate training will be provided to those staff for whom it has been decided that access is required.

The Business Manager or Facilities/Premises/Site Manager will arrange for introductory and familiarisation training, in the use of the system, to all personnel required to operate the CCTV system. The systems may vary between academies.

Staff will receive training and will be required to demonstrate competence in:

- The purpose of the system as defined by this policy
- The rights of individuals under the CCTV system
- Data Protection / Freedom of Information Policy
- Equipment use
- Recognition of the privacy implications of the visual area to be covered
- Recognition that images must only be viewed by authorised employees of the academy/trust.