



THE CONSORTIUM
ACADEMY TRUST

Shaping Positive Futures

CCTV Policy

The Consortium Academy Trust (TCAT)
An Exempt Charity Limited by Guarantee
Company Number 07665828

Status:	Live
Policy Owner (position)	DPO and Director of Infrastructure
Statutory / Recommended	Recommended
Date Adopted	16 July 2018
Revision	4
Last Review Date	May 2025
JCNC Consultation Date	December 2023, 10 July 2025
Review Period	24 months
Next Review Date	July 2027
Advisory Committee	Trust Board
Linked Documents and Policies	Data Protection Policy Freedom of Information Guidance ICT Acceptable Use Policy and Records Management Policy

**NB – This document can only be considered valid when viewed on The Consortium Academy Trust website. If the copy is printed or downloaded and saved elsewhere the Policy date should be cross referenced to ensure the current document is the latest version. The linked policies can be found at www.consortiumtrust.co.uk*

CONTENTS

POLICY STATEMENT

- 1.0 Why the Policy is Needed
- 2.0 What the Policy is About
- 3.0 What the Policy Will Achieve

PROCEDURE

- 1.0 Legal framework
- 2.0 Definitions
- 3.0 Roles and Responsibilities
- 4.0 Location of Cameras
- 5.0 Purpose and Justification
- 6.0 Protocols
- 7.0 Security and Retention
- 8.0 Access to Footage
- 9.0 Viewing by Third Parties
- 10.0 Additional Information

Appendices:

- 1. Internal Signage
- 2. External Signage
- 3. Access Flowchart

POLICY STATEMENT

1.0 Why the Policy is Needed

The Consortium Academy Trust (“the Trust”) takes the responsibility towards the safety of learners, staff and visitors very seriously. It is important that these stakeholders feel safe in their learning and working environments – this is aligned to two of our values of respect and responsibility.

One method of keeping individuals and our environments safe is through the appropriate use of surveillance where at times we may need to recall any instances of disrespectful behaviour which has led to individuals being harmed or property being damaged. CCTV systems can also act as a deterrent of such behaviour.

2.0 What the Policy is About

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified and includes information recorded using any of the Trust’s swipe cards and time recording facilities.

This policy should be read in conjunction with the related Trust policies listed on the front page.

3.0 What the Policy Will Achieve

The purpose of this policy is to manage and regulate the use of the surveillance and Closed-Circuit Television (CCTV) systems used by the Trust and ensure that:

- we comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).
- the images that are captured are useable for the purposes we require them for.
- we reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

CCTV PROCEDURE

1.0 LEGAL FRAMEWORK

This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- UK GDPR
- Data Protection Act 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2021) Guide to the UK General Data Protection Regulation (UK GDPR)
- ICO (2022) Surveillance Guidance
- DfE (2022) Protection of Biometric Data of Children in Schools and Colleges

This policy operates in conjunction with the following Trust policies:

- Data Protection Policy
- Freedom of Information Policy
- Online Safety Policy

2.0 DEFINITIONS

For the purpose of this policy the following definitions shall have the following meanings:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio, live footage. For the purpose of this policy only video footage will be applicable.
- Overt Surveillance – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000
- Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The Trust does not condone the use of covert surveillance when monitoring each school's staff, learners and/or visitors.

3.0 ROLES AND RESPONSIBILITIES

The Trust is responsible for:

- dealing with freedom of information requests and Data Subject Access Requests (DSAR) in line with legislation.
- ensuring that each school handles and processes surveillance and CCTV footage in accordance with data protection legislation.
- ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- informing data subjects of how their data captured in surveillance and CCTV footage will be used by the Trust, their rights for the data to be destroyed and the measures implemented by the Trust to protect individuals' personal information.

The Trust, as the corporate body, is the data controller.

The DPO for the Trust is based at the Trust's headquarters at Cottingham High School and whose email address is **dpo@consortiumtrust.co.uk**. The DPO has responsibility for overseeing the operation of this policy.

Each school has a Data Protection Link who is available for any concerns / queries about CCTV.

4.0 LOCATION OF CAMERAS

The Trust operates a CCTV surveillance system at all of its schools.

The Trust operates video entry systems at some of its schools.

None of the systems record audio footage.

Robertsons Facilities Management manage the CCTV system at Winifred Holtby Academy and will comply with this policy.

5.0 PURPOSE AND JUSTIFICATION

The Trust uses surveillance footage in order to:

- maintain a safe environment at each school
- ensure the welfare of learners, staff, volunteers and visitors
- behaviour management
- deter and detect criminal acts against persons and property
- assist the police / Local Authority Designated Officer (LADO) with any concerns
- assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- assist in the defence of any litigation proceedings

The Trust has considered alternatives to using CCTV, such as additional regular inspections of its premises, but has concluded that such alternatives would be less effective and more costly. In particular, there are situations that require a rapid response if the risk to learners', staff and visitors' security and safety is to be minimised. CCTV is the best way for the Trust to achieve this.

The Trust reserves the right to use CCTV footage in connection with any disciplinary action or other proceedings.

Under no circumstances will the surveillance and the CCTV cameras be present in any changing facility.

Cameras may be present in wash areas, provided that cameras are not directed to cubicles or urinals and there is a justified reason to have cameras present, such as to deter vandalism and ensure safety of learners.

CCTV cameras will only be present in classrooms with the agreement and prior knowledge of the Headteacher and DPO, following a Data Protection Impact Assessment (DPIA). The cameras will not be in classrooms to monitor teaching and learning, but to deter vandalism, theft or poor behaviour.

The system will **not** be used:

- to provide recorded footage for the internet
- for any commercial or entertainment purpose
- for any automated decision taking
- to monitor teaching and learning
- in any meeting rooms/ social areas

6.0 PROTOCOLS

The Trust has registered that it operates a CCTV surveillance system with the ICO in line with data protection legislation.

Data collected from CCTV will be:

- Processed lawfully, fairly and limited to what is necessary in relation to the purposes for which they are processed
- Collected for legitimate purposes, data will not be processed further

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. A related Privacy Statement explaining the Trust's use of the system (as required by the UK GDPR) has been posted online by the Trust and this website address is stated on each sign.

Footage recorded using each school's CCTV system is recorded at the relevant school.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of any school.

7.0 SECURITY AND RETENTION

Access to the surveillance system, software and data (including visual display monitors) is strictly limited to authorised operators as designated by the relevant school and will be password protected.

CCTV will not be displayed on constant large format displays or on live view.

The Headteacher will approve who is an “authorised user” and any request to add users to the list must be authorised by the Headteacher.

The ICT team will install updates to software and operating systems in line with manufacturer guidelines and will have monthly preventive maintenance tasks to ensure the system is fully operational.

Only authorised users are permitted to access the footage. If a member of staff needs to view footage for an approved purpose, then they need to approach a CCTV authorised user – see section 8.

The main control facility at each school is kept secure and locked when not in use.

Each school will have a separate system that can be run independently of one another.

Any cameras that present faults will be repaired as soon as is reasonably practicable as to avoid any risk of a data breach.

Footage will not be removed from the system itself other than in accordance with this policy. All footage recorded using the systems will be retained for up to 30 days from the date of the recording and then automatically overwritten. Any footage copied from the system for a purpose set out in this policy will be retained for a reasonable period (determined by the DPO) having regard to the reason for copying the footage.

8.0 ACCESS TO FOOTAGE (please see flowchart on page 11 of this policy)

Internal requests - may be made by any member of Trust staff for any of the approved purposes listed in section 5.

If a staff member needs to view footage for any of the reasons listed in 5.1, they need to request to view the footage with an authorised user.

The authorised user **must** complete the Internal Viewing record form for all requests

External requests are third party requests (i.e. not a member of staff). All external requests to view and disclose CCTV footage must be recorded in the relevant school’s data protection database by the school Data Protection Link. Such records must include details of the accessor / recipient of the footage and the date and reason for the access / disclosure.

All requests for access to footage (including but not limited to requests from law enforcement agencies and DSARs) will be at the discretion of an authorised user. No such footage shall be disclosed to any third party or unauthorised employee without specific authorisation from the Headteacher and DPO. If the Headteacher approves the request, this needs to be confirmed by the DPO by emailing dpo@consortiumtrust.co.uk. Any such disclosure should be proportionate having regard to the purpose of the footage being requested (e.g. if a law enforcement agency asks to see footage of an incident which occurred at a specific time, the amount of footage disclosed should be limited to footage from around that time).

In the event that any footage is provided to law enforcement agencies, this shall be by making it available for them to view at the relevant Trust premises unless otherwise authorised by the DPO.

Any DSAR for CCTV footage will be handled in accordance with the Trust’s Data Protection Policy and the request will be logged on the central data protection database.

9.0 VIEWING BY THIRD PARTIES

Every effort should be made to encourage third parties to come on site to view the footage. Faces need to be blurred or written consent of those involved must be sought prior to viewing.

If third parties request that footage is shared as they cannot come on site, then the footage should be put on a secure platform with the download disabled. The recipient should be informed that they are now the data controller, and it is their responsibility to keep the data safe and not share it further.

Requests by the police to view CCTV should be detailed on a DP9 (official police document). **Viewing cannot be granted without this form.**

Releasing the recorded images to the following third parties will be permitted to the extent required or permitted by law:

- The police – where images would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Legal representatives – such as lawyers and barristers
- Data subjects who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation

Any request to view CCTV by a union representative should be made in writing to the Headteacher. The Headteacher will review the request and allocate an authorised user to show the footage to the union representative if the request is permitted.

10.0 ADDITIONAL INFORMATION

This policy does not form part of any employee's contract of employment, and it may be amended by the Trust at any time, after consultation with the recognised trade unions.

If you are found to be in breach of the terms of this policy you may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal (and, in exceptional circumstances, criminal charges). If you are in any doubt about the terms of this policy or have any questions or complaints in relation to the Trust's CCTV systems or the operation of this policy, please contact the DPO at dpo@consortiumtrust.co.uk.

1.0 Example of Internal Signage

WARNING



CCTV cameras in operation

This site is protected by CCTV for the purposes of site security and preventing and detecting crime. The CCTV system is operated by The Consortium Academy Trust (Tel - 01482 469838). For further information please visit www.consortiumtrust.co.uk/statutory



THE CONSORTIUM
ACADEMY TRUST

WARNING



**CCTV cameras
in operation**

This site is protected by CCTV for the purposes of site security and preventing and detecting crime. The CCTV system is operated by The Consortium Academy Trust (Tel - 01482 469838). For further information please visit www.consortiumtrust.co.uk/statutory

**Users of this car park
do so at their own risk**



THE CONSORTIUM
ACADEMY TRUST

3.0 CCTV Access Flowchart

