



Broadway Academy Policies

Our Children. Our Community. Believe it can be done!

CCTV Policy

Approved by: Finance, Audit and Premises Committee

Date approved: June 2025

Next review date: June 2027



Contents

	Section	Page
1	Introduction	2
2	Objectives of the CCTV Policy	2
3	Principles	3
4	The Data Protection Principles	3
5	Operational Control & Protocols	4
6	Monitoring Procedures	5
7	Recorded Material Procedures	5
8	Record Keeping / Incident Logs	6
9	Retention of Data	6
10	Security	6
11	Data Protection Impact Assessment (DPIA)	6
12	Breaches of the Policy	7
13	Assessment of the CCTV System	7
14	Access by the Data Subject	7
15	Complaints	7
16	Further Information	8

1. Introduction

- 1.1 The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Broadway Academy hereafter referred to as 'the Academy'.
- 1.2 The CCTV system is owned by the Academy. The system comprises a Hickman IP system with 72 cameras which provide whole site cover of the Academy's external and internal areas (apart from the toilets, changing rooms and staff rooms). System control is managed by the Director of Site and Facilities Management.
- 1.3 On a day-to-day basis, cameras are monitored by the Director of Site and Facilities Management and the site security staff. Recorded images from any camera can only be accessed with express permission from the Head Teacher or the Director of Site and Facilities Management.
- 1.4 The system will not be used for any other purpose than those set out in this document without prior consultation with the Head Teacher, and where appropriate, notification to staff.
- 1.5 This Policy has been drafted in compliance with the requirements of the General Data Protection Regulation (GDPR).
- 1.6 The ongoing suitability of the Academy CCTV Policy will be reviewed biannually by the Academy Governing Body.

2. Objectives of the CCTV Policy

- 2.1 This Policy covers the use of CCTV systems, which capture moving and still images of people who could be identified, for the following purposes:
 - To protect academy buildings, grounds and their assets within
 - To increase personal safety of those within, and visiting the Academy community
 - To act as a deterrent for violent behaviour and damage to the Academy
 - To support the Police to deter and detect crime
 - To assist in identifying, apprehending and disciplining offenders
 - To determine the cause of accidents
 - To assist in the investigation of suspected breaches of conduct or standards by staff or students
 - Assist in the defence of any litigation proceedings

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

- 2.2 This policy has been created with regard to the following statutory and non-statutory guidance:
 - Information Commissioner's Office (ICO) (2024) 'Video Surveillance (including guidance for organisations using CCTV)'
 - Biometrics and Surveillance Camera commissioner (Gov) (2022) Update to Surveillance Camera Code of Practice - GOV.UK (www.gov.uk)
- 2.3 This policy has due regard to legislation including the following:
 - The General Data Protection Regulation
 - The Data Protection Act 2018
 - The Freedom of Information Act 2000
 - The Protection of Freedoms Act 2012

- The Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- The Schools Standards and Framework Act 1998
- The Equality Act 2010
- The Children Act 2004
- Human Rights Act 2018
- European Convention of Human Rights

This policy operates in connection with the following school policies:

- Data Protection Policy
- Freedom of Information Policy
- Child Protection and Safeguarding Policy
- Privacy notices for Pupils, Parents and Carers
- Privacy Notice for School Staff
- Privacy Notice for Visitors and Contractors
- Privacy Notice for Governors

3. Principles

- 3.1 The Academy will treat the system and all information, documents and recordings obtained and used as data protected by the GDPR, and which will be processed in accordance with the requirements of the regulation.
- 3.2 Cameras will be used to monitor activities within the internal and external areas of the Academy buildings and grounds in line with the objectives at 2.1. Cameras are located on corridors in student areas of the school, in the dining and sports halls, on front reception and in the car parks.
- 3.3 The Academy will only operate overt surveillance and will display signs in the areas of the Academy where this is in operation. Covert surveillance (i.e. which is intentionally not shared with the individuals being recorded) is not condoned by the Academy.
However, if the situation arises where covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.
- 3.4 Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the Academy CCTV.
- 3.5 The CCTV system will not be trained on individuals unless an immediate response to an incident is required.
- 3.6 The CCTV system will not be trained on private vehicles or property outside the perimeter of the Academy.

4. The Data Protection Principles

- 4.1 Data collected from CCTV will be processed in accordance with the principles of the General Data Protection Regulation. As such, all data will be:
 - a) Processed lawfully, fairly and in a transparent manner in relation to individuals
 - b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
 - c) Adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed
 - d) Accurate and where necessary, kept up to date

- e) Kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data are processed
- f) Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

5. Operational Control and Protocols

- 5.1 Access to the CCTV system, software and data, will be strictly limited to authorised operators and is password protected.
- 5.2 The responsibility for the leadership and management of the CCTV system is that of the Head Teacher and CEO.
- 5.3 The system will be managed by the Director of Site and Facilities Management in accordance with the principles and objectives expressed in this policy.
- 5.4 The day-to-day administration of the system will be the responsibility of Director of Site and Facilities Management and Community Centre Managers during the day, out of hours and at weekends.
- 5.5 The CCTV system will be operated as a live recording system 24 hours a day every day of the year. The system will not record audio.
- 5.6 The Operational Controller will check and confirm the efficiency of the system once per month and, to confirm that the equipment is properly recording and that cameras are functional.
- 5.7 The System Administrator will ensure that **all** staff involved with the operation of the CCTV system are properly trained and fully understand their roles and responsibilities in respect of data protection issues e.g.
 - the user's security policy (procedures to have access to recorded images)
 - the user's disclosure policy
 - rights of individuals in relation to their recorded images.Training records will be maintained accordingly.
- 5.8 Access to the CCTV viewing monitors situated in reception will be limited to Security and Community staff, as well as those directly involved in the security of the Academy. Staff monitoring the system will have SIA training and CCTV licences, individual logins and have undergone appropriate training.
- 5.9 A CCTV viewing permission form must be completed and authorised by Director of Site and Facilities Management or the Headteacher and CEO, before any other parties can view the CCTV footage. A log of all viewing is kept.
- 5.10 The CCTV monitors are located in a secure area behind a coded door. Staff, visitors and others entering areas with CCTV viewing monitors will be subject to arrangement as outlined below.
- 5.11 Authorised staff must satisfy themselves over the identity of any other visitors and the purpose of their visit. Where any doubt exists, the CCTV monitors must be turned off.
- 5.12 It is vital that operations are managed with the minimum of disruption. Casual observations will not be permitted.

- 5.13 If an emergency arises out of hours, permission must be obtained from the Headteacher and CEO to view or process recorded material.
- 5.14 Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.
- 5.15 Incidents involving the Emergency Services must be notified to Bal Braich, Director of Site and Facilities Management.

6. Monitoring Procedures

- 6.1 Camera surveillance may be maintained at all times.
- 6.2 Pictures will be continuously recorded.
- 6.3 No covert monitoring will be undertaken until the circumstances have been considered by, and written authorisation obtained from the Headteacher.

7. Recorded Material Procedures

- 7.1 In order to maintain and preserve the integrity of the recorded material used to record events from the CCTV system, and the facility to use them in any future proceedings, the following procedures for their use and retention **must** be strictly adhered to:
- a) Each item of recorded material must be identified by a unique mark.
 - b) The system will register the date and time of recorded material insert, including recorded material reference.
 - c) Any recorded material required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure recorded material store. If recorded material is not copied for the Police before it is sealed, a copy may be made later providing that it is then resealed, witnessed, signed by the Controller, dated and returned to the evidence material store.
 - d) If the recorded material is archived the reference must be noted.
- 7.2 Recorded materials may be viewed by or released to third parties in the following prescribed circumstances, and then only to the extent required by law or statutory guidance:
- The police, where any images recorded would assist in a specific criminal inquiry
 - Prosecution agencies, such as the Crown Prosecution Service (CPS)
 - Relevant legal representatives such as lawyers and barristers
 - Insurance companies where images may be required to process a potential liability claim
 - Persons whose images have been recorded and retained, and where disclosure is required by virtue of data protection legislation, or the Freedom of Information Act.
 - Where a suspicion of misconduct arises and at the formal request of the Head Teacher access may be provided to CCTV images for use in staff disciplinary cases, including disclosure to legitimate third parties (such as external investigators or nominated representatives)
- 7.3 A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register, maintained by the Controller will be made available for this purpose.

- 7.4 Viewing of recorded materials by the Police must be recorded in writing and in a logbook.
- 7.5 Should recorded material be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1(iii). Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the Academy, and both the recorded material and information contained on it are to be treated in accordance with this document.
- 7.6 The Academy retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material this will be produced from the secure recorded material store, complete in its sealed bag.
- 7.7 If the Police require the Academy to retain the stored recorded materials for use as evidence in the future, such recorded materials will be properly indexed and properly and securely stored until they are needed by the Police.
- 7.8 Requests for any access or disclosure will be recorded and the Head Teacher and CEO will make the final decision as to whether the recorded images may be released to persons other than the police.

8. Record Keeping / Incident Logs

- 8.1 The Academy will maintain adequate and comprehensive records relating to the Management of the system and incidents. Model documents from the installers/providers of CCTV system may be utilised for this purpose.

9. Retention of Data

- 9.1 The system data retention period will be for 90 days.
- 9.2 Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.
- 9.3 Measures to permanently delete data should be clearly understood by persons that operate the system.
- 9.4 Systematic checks should be carried out to ensure the deletion regime is strictly followed.

10. Security

- 10.1 All devices used are encrypted so that CCTV footage is stored securely at all times. Access to footage will be via password by authorised personnel only.
- 10.2 Security measures are in place to protect all footage from potential cyber-attacks.

11. Data Protection Impact Assessments

- 11.1 Where changes to the CCTV system are made such as additional cameras being installed or moved to other areas on site, or a complete replacement, a Data Protection Impact Assessment (DPIA) will be carried out. This will identify potential risks to data by replacing or developing the system as well as to ensure

the system remains justifiable, necessary and proportionate in line with the GDPR.

- 11.2 The Academy's DPO will provide guidance and appropriate paperwork required to capture proposals and considerations made and to identify potential risk and safeguards needed. The completion of the DPIA will be led by the Strategic IT Director.

12. Breaches of the Policy (including breaches of security)

- 12.1 Any breach of the Policy by Academy staff will be initially investigated by the Head Teacher and CEO or his nominee to determine action, if necessary, and to make recommendations on how to remedy the breach in liaison with the Academy's Data Protection Officer.

13. Assessment of the CCTV System

- 13.1 An annual assessment will be undertaken by the Head Teacher and CEO to evaluate the effectiveness of the CCTV system. The outcome of the assessment will be reported to a meeting of the Academy Governors who will determine if the system is achieving the objectives of the scheme, or if the system requires modification.

14. Access by the Data Subject

- 14.1 The GDPR provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV.
- 14.2 Individuals have the right to submit a subject access request to gain access to their personal data. Access to CCTV footage will be dealt with in line with the Academy's Data Protection Policy and subject access request process.
- 14.3 If the data subject is not the focus of the footage i.e. there are more individuals visible, or they have not been singled out or had their movements tracked then the images are not classed as 'personal data' and the individual is not entitled to the image under the provisions of Subject Access Requests.
- 14.4 In such instances, the Academy will verify the identity of the individual making the request before any information is provided.
- 14.5 All requests will be responded to without delay, and at the most within one calendar month.
- 14.6 Requests for access or disclosure will be recorded and the Head Teacher and CEO will make a final decision as to whether recorded images may be released to persons other than the police.
- 14.7 Further guidance can be found in the Academy's procedure for responding to subject access requests in the Data Protection Policy.

15. Complaints

- 15.1 Any complaints about the CCTV system should firstly be made, in writing, to the Head Teacher and CEO. Complaints will be investigated in accordance with section 14.

- 15.2 If an individual is dissatisfied with the assistance that they have received from the school they can contact the schools Data Protection Officer at gdpr@sips.co.uk or on telephone number 0121 296 300. A formal complaint can also be made to the Information Commissioners Office who is an independent regulator. This can be done via the website at www.ico.org.uk; Telephone: 0303 123 1113; or in writing to: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A.

16. Further Information

- 16.1 Further information on data protection issues related to CCTV may be obtained from Bal Braich, Director of Site and Facilities Management
bal.braich@broadway-academy.co.uk
- 16.2 The Data Protection Officer role is provided for the Academy by SIPS Education and queries should be referred to gdpr@sipseducation.co.uk or 0121 296 3000.
- 16.3 The Information Commissioners website www.ico.gov.uk will contain the most up to date information and should be consulted on a regular basis to ensure all elements of this policy continue to reflect current guidance.