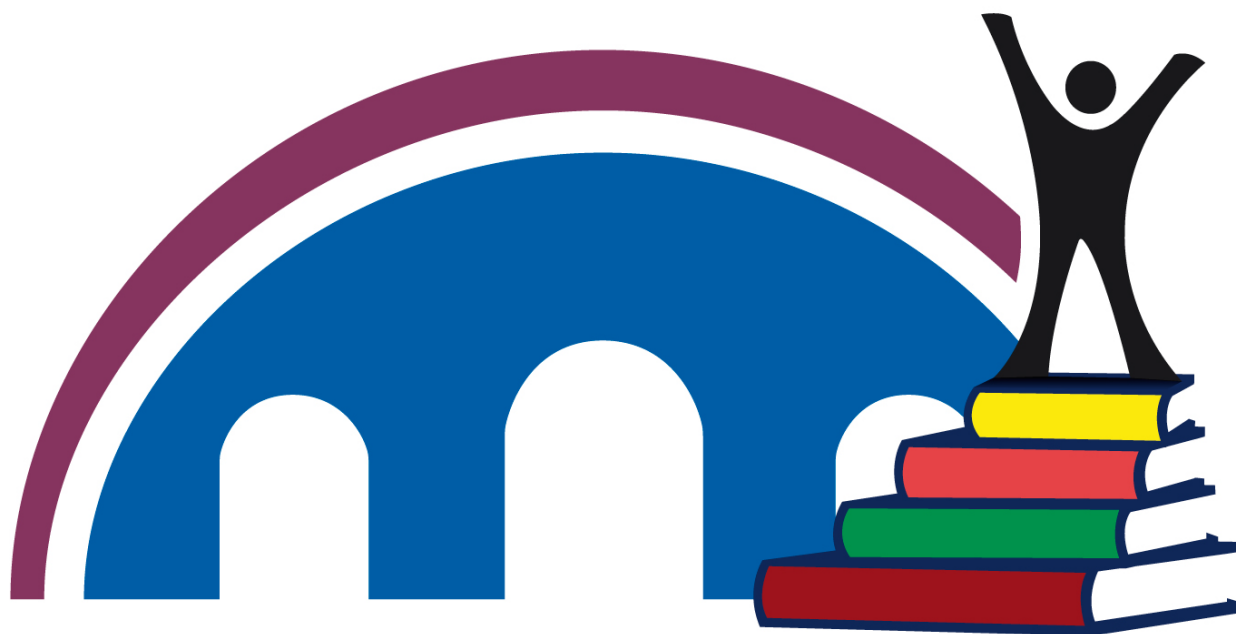




Bridge Academy Trust

CCTV POLICY

September 2026

Summary of Changes

Section Number	Current	Proposed Amendment
2: Scope	N/A	New section added.
3. Roles and Responsibilities	N/A	New section added.
4. Equality and Impact Assessment	N/A	New section added.

Date of Draft Policy: (this is the month/year the policy was drafted)	March 2026	
Last approved version Frequency of review	March 2025 Annually	
Consultation with Staff Required	Yes ☐	No ☒
Period of Consultation (if required)	From N/A	To N/A
Trustees Committee Reviewing Document	Trustee Policy Review Committee	
Date of Board of Trustees Meeting at which Policy Approved	16 th June 2026	
Date of Adoption of Policy	1 st September 2026	
Date Policy available on Central Area/www (If appropriate)	1 st September 2026	
Reviewer	Data Protection Officer (DPO)	
Advice From	Information Commissioner's Office (ICO)	

Contents

INTRODUCTION	1
SCOPE	1
ROLES AND RESPONSIBILITIES	1
BRIDGE ACADEMY TRUST (as Data Controller)	1
HEADTEACHER/HEAD OF SCHOOL	1
DATA PROTECTION OFFICER (DPO).....	2
IT TEAM.....	2
SITE TEAM/AUTHORISED STAFF	2
ALL STAFF	2
EQUALITY IMPACT ASSESSMENT (EIA)	2
STATEMENT OF INTENT	3
PLACEMENT OF CAMERAS	3
STORAGE AND RETENTION OF CCTV IMAGES	4
ACCESS TO CCTV IMAGES	4
ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES.....	4
SUBJECT ACCESS REQUESTS (SARS)	5
COMPLAINTS	5
DPO CONTACT DETAILS.....	5
APPENDIX A.....	Error! Bookmark not defined.
APPENDIX B	Error! Bookmark not defined.

INTRODUCTION

- 1.1 Bridge Academy Trust uses closed circuit television (CCTV) images to reduce crime and monitor school buildings to provide a safe and secure environment for pupils, staff, visitors and to prevent the loss or damage to school property.
- 1.2 The system comprises of several fixed cameras and in some schools the system has sound recording capability.
- 1.3 The CCTV system is owned and operated by the Trust, the deployment of which is determined by the school's leadership team.
- 1.4 The CCTV is monitored by the Site Team, the DPO (Data Protection Officer), IT staff and any other relevant staff.
- 1.5 The school's CCTV scheme is registered with the Information Commissioner's Office under the relevant legislation. The use of CCTV and the associated images and any recording is covered by the relevant legislation. This policy outlines the Trust's use of CCTV and how it complies with the act.
- 1.6 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 IT Staff or have Data Protection responsibilities within their roles. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.
- 1.7 Other staff may have access to the CCTV system at the discretion of the Headteacher/Head of School.

SCOPE

- 2.1 This policy applies to all Bridge Academy Trust schools, central teams, staff, pupils, contractors, and visitors who may be captured by the Trust's CCTV systems.

ROLES AND RESPONSIBILITIES

BRIDGE ACADEMY TRUST (AS DATA CONTROLLER)

- 3.1 Bridge Academy Trust is responsible for:
 - a) Overall responsibility for ensuring CCTV systems across all schools comply with data protection legislation and ICO video surveillance guidance.
 - b) Ensures each school operates CCTV in accordance with this policy and Trust wide standards.

HEADTEACHER/HEAD OF SCHOOL

- 3.2 The Headteacher/Head of School has delegated responsibility to:
 - a) Oversee the day-to-day operation of CCTV within their school.
 - b) Authorises staff access to CCTV footage and ensures appropriate controls are in place.

- c) Ensures signage, camera placement, and local procedures meet Trust and legal requirements.

DATA PROTECTION OFFICER (DPO)

3.3 The Data Protection Officer (DPO)

- a) Provides advice on lawful operation of CCTV and ensures compliance with data protection laws.
- b) Handles Subject Access Requests (SARs) and third-party disclosure requests.
- c) Reviews, audits, and monitors CCTV practices across the Trust.

IT TEAM

3.4 The IT Team:

- a) Maintains the technical operation, security, and integrity of CCTV systems.
- b) Ensures systems are password-protected, securely configured, and retention settings are correctly applied.
- c) Supports schools with access, troubleshooting, and secure storage of footage.

SITE TEAM/AUTHORISED STAFF

3.5 The Site Team/Authorised Staff:

- a) Monitor live feeds (where applicable) and access recordings for legitimate purposes only.
- b) Record all access in the CCTV access log, including time, date, and reason.
- c) Report faults or security concerns to IT and the Headteacher/Head of School.

ALL STAFF

3.6 All Staff:

- a) Must follow this policy and only request CCTV footage for legitimate, authorised reasons.
- b) Report any concerns or breaches immediately to the Headteacher/Head of School or the DPO.

EQUALITY IMPACT ASSESSMENT (EIA)

- 4.1 An Equality Impact Assessment has been completed for this policy and has identified no significant negative impacts.

STATEMENT OF INTENT

- 5.1 The Trust complies with the guidance published by the Information Commissioner's Office (ICO) relating to CCTV to ensure it is used responsibly and to safeguard both the trust and maintain confidence in its continued use. The guidance is available from the ICO website: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance/>
- 5.2 The planning and design have endeavoured to ensure 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.
- 5.3 The purpose of the CCTV system is to (this is not an exhaustive list, and other purposes may be or become relevant):
- a) Make members of the school community feel safe.
 - b) Protect members of the school community from harm to themselves or to their property.
 - c) Deter criminality in the school.
 - d) Protect school assets and buildings.
 - e) Assist Police to deter and detect crime.
 - f) Determine the causes of accidents.
 - g) Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings.
 - h) To assist in the defence of any litigation proceedings.
- 5.4 The CCTV will not be used for (this is not an exhaustive list, and other purposes may be or become relevant):
- a) Encroach on an individual's right for privacy.
 - b) Monitor people in spaces where they have a heightened expectation of privacy.
 - c) Follow particular individuals, unless there is an ongoing emergency incident occurring.

PLACEMENT OF CAMERAS

- 6.1 Cameras are placed so as to only capture images relevant to the purpose for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The trust will ensure that the location of equipment is carefully considered to ensure that images captured comply with any relevant legislation.
- 6.2 Bridge Academy Trust will make every effort to position cameras so that coverage is restricted to the school premises, which may include outdoor areas.
- 6.3 CCTV will not be used in general purpose classrooms. CCTV will be allowed to be used in IT rooms to help prevent any loss or damage to school IT equipment. It will also be used in corridors, stairs, outdoor areas, and any other areas that are felt appropriate by the school.

STORAGE AND RETENTION OF CCTV IMAGES

- 7.1 All retained data will be stored securely.
- 7.2 Recorded data will not be retained for longer than necessary. When 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.
- 7.3 Footage will be retained for 30 days. At the end of the retention period, the files will be automatically overwritten.
- 7.4 Footage retained for internal investigations will be retained for 60 days. At the end of the retention period, the files will be deleted.

ACCESS TO CCTV IMAGES

- 8.1 Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.
- 8.2 Authorised staff will be able to remotely access CCTV via the website or using a mobile app if it is supported by the school's CCTV System. Access rights to the systems will be password protected.
- 8.3 Any staff member who accesses the CCTV system must record their name, the date and time and the reason for access in the access log.
- 8.4 When accessing CCTV footage relating to students, staff are to seek permission from either Deputy Headteacher, Designated Safeguarding Lead or Headteacher/Head of School. If these people are unavailable to authorise the request and there is an urgent need to access the footage, the Trust Data Protection Officer can authorise the request.
- 8.5 Authorisation to access the CCTV footage relating to students is granted on a case-by-case basis.

ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

- 9.1 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 trust where these need access to the data.
- 9.2 Requests should be made in writing to the DPO.
- 9.3 The data may be used within the trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.
- 9.4 The Trust will comply with any court orders that grant access to the CCTV footage. The Trust will provide the courts with the footage they need without giving unrestricted access. The Data Protection Officer will consider very carefully how much footage to disclose and seek legal advice if necessary.

SUBJECT ACCESS REQUESTS (SARS)

- 10.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection legislation.
- 10.2 All requests should be made in writing to the Data Protection Officer. 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.
- 10.3 The Trust 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.

COMPLAINTS

- 11.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance as per the Complaints Policy.

DPO CONTACT DETAILS

Mr. Kieran Saul
dpo@bridgeacademytrust.org