CLOSED CIRCUIT TELEVISION (CCTV) POLICY AND PROCEDURE

Author:	Head of Operations - DPO
Approved by:	CEO
Date:	December 2025
Review date:	Dec 2027

Contents

1 Introduction

1.1 The Bridgwater and Taunton College Trust (BTCT) is fully committed to operating a safe environment, and one means of achieving this is by the use of closed circuit television (CCTV) surveillance to provide a safe and secure environment for students, staff, visitors and to protect Trust property.

2 Scope

2.1 The Trust has produced this policy and procedures in line with the Information Commissioner's CCTV Code of Practice, Home Office Surveillance Camera Code of Practice, and to also ensure the Trust complies with the Data Protection Act 2018, General Data Protection Regulation (GDPR), Human Rights Act 1998 and other relevant legislation.

2.2 The Trust is registered with the Information Commissioner's Office (ICO) Registration number ZA169178

3 CCTV System Overview

3.1 The system comprises: fixed position cameras, pan, tilt and zoom cameras, dome cameras and viewing equipment including monitors, recording media, non audio and public information signs in building and in Trust Vehicles designed to carry pupils.

3.2 The CCTV system is owned by Bridgwater and Taunton College Trust and is managed by the Trust and its appointed agents.

3.3 The Data Controller is responsible for the operation of the system and for ensuring compliance with this policy and its procedures.

3.4 The Data Controller is:

The CEO
Bridgwater and Taunton Trust
Parkway
Bridgwater
Somerset
TA6 4

3.5 The Data Controller delegates responsibility for the day to day operation of this policy and its procedures to the Trust's Data Protection Officer.

3.6 The CCTV system operates across all campuses and is capable of being monitored 24/7, all year round.

3.7 Cameras are sited to ensure that they only cover the Trust's premises. Cameras are installed throughout the Trusts sites including: entrance roads, pedestrian entrance/s to sites and buildings, car parks, buildings both internally and externally and residential accommodation and vehicles.

3.8 Cameras are sited so as not to include any private residential areas around the campuses sites. Cameras within the Trust's own residential accommodation focus on entrance doors and communal areas only.

3.9 Signs are placed at entrances to trust sites in order to inform staff, students, visitors, contractors and member of the public that CCTV is in operation and its purpose and contact details for further information, if required.

3.10 The Trust will carry out a data protection impact assessment (DPIA) on the surveillance camera system every 12 months or as and when changes are made to the CCTV system (see Appendix 1 Data Protection Impact Assessment for surveillance cameras).

4 Purposes of the CCTV System

4.1 The principal purpose of the Trust's CCTV system are as follows:

- The system is operated for the prevention, deterrence and detection of crime, including the safeguarding of individuals, and to support the effective management of the Trust's sites
- To ensure the provision of a safe and secure environment for pupils, staff, visitors and Trust property.
- To assist in the investigation of suspected breaches of Trust regulations

Note - reviewing CCTV is a time consuming and therefore expensive activity and will only be complete when proportionate to what is being explored.

4.2 The CCTV system will be used to observe relevant areas of the Trust's sites and areas under surveillance to identify any incidents and to take appropriate action which is proportionate to the incident being witnessed.

4.3 The Trust seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

5 Monitoring and Recording

5.1 Cameras are monitored by authorised Trust staff and/or appointed agents only (see Appendix 2). Authorisation can only be given by the Data Controller and/or Data Protection Officer.
Details of named individuals who are authorised to view the CCTV system are held by Data Protection Officer. To obtain authorisation to view CCTV, a Request Record of Viewing CCTV Data Form (see Appendix 3) must be submitted to the Data Protection Officer and authorised before viewing any CCTV images, in an emergency or time critical situation where the purposes are in line with (4.1) and authorisation can then be sought retrospectively with an assessment completed of that requirement by the DPO.
Authorised staff may request a relevant person to view the image with them to confirm an individual's identity etc. and details of this person who viewed the image with the authorised person and why they were requested to view the image must be recorded on the form. Under no circumstances should any other person(s) be able to view the images.

The viewing of live images on monitors is restricted to authorised system users only unless the monitor displays a scene which is in clear sight from the monitor location.

5.2 Images captured by the system may be monitored and recorded on to the Trust's servers on a loop of 28 days before being over written throughout the whole year. Recorded material will be stored in a way to maintain the integrity of the image to ensure that the rights of individuals recorded by the system are protected and that the material can be re-produced to be used for authorised purposes.

5.3 All images recorded by the CCTV system remain the property and copyright of Bridgwater & Taunton College Trust.

5.4 Covert cameras will be restricted to specific occasions, when a series of criminal acts or breaches of Trust rules have taken place within a particular area of a campus that is not already covered by CCTV.

5.5 A request for the use of covert camera/s must be submitted to the Data Protection Officer clearly stating the name of the person making the request, the purpose and the reason for the proposed monitoring (see Appendix 4). A Data Impact Assessment for Surveillance Cameras (see Appendix 1) must also be completed before authorisation. Only when authorised, may the covert camera/s be installed.

5.6 The use of covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there is reasonable grounds to suspect that illegal or unauthorised activity is taking place.

5.7 Any such monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring, and only for a specific unauthorised activity.

5.8 Systematic checks are carried out to ensure that the quality of images being recorded is upheld and the accuracy of the time/date stamp is maintained.

5.9 Recorded images will only be viewed in a secure area by staff authorised by the Data Controller/Data Protection Officer to do so, to ensure that no unauthorised persons are able to view the image.

5.10 All completed forms are to be forwarded to the Data Protection Officer. It is planned to digitise the forms in the near future to simplify the process.

5.11 A robust monthly audit check will be carried out to ensure only permitted user access to the system has been authorised.

5.12 CCTV footage can only be viewed without authorisation in an emergency or time critical situation where the purposes are in line with (4.1) and authorisation can then be sought retrospectively with an assessment completed of that requirement by the DPO.

6 Compliance with Data Protection Regulations/GDPR

6.1 In its administration of its CCTV, the Trust complies with the Data Protection Act 1998 and General Data Protection Regulation, the principles of which state that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed
- Accurate, and where necessary kept up to date
- Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
- Kept for no longer than necessary for the particular purpose
- Processed in accordance with the rights of individuals

7 Access by Individual Data Subjects

7.1 Anyone who believes they have been filmed by CCTV is entitled to ask for a copy of their images, subject to the prohibitions on access also covered by GDPR. They do not have the right of instant access and must abide by the Data Protection Procedures. The Individual should submit their request on a Data Subject Access Request Form (Appendix 5) to the Trusts Data Protection Officer.

7.2 Requests for access to CCTV images must include:

- The reason for the request
- The date and time that the images requested were recorded
- Information to be able to identify the individual, if necessary
- The location of the CCTV camera
- Proof of identity

7.3 The Trust will respond promptly and at the latest within 20 working days of receiving the request and if provided with sufficient information to be able to identify the images requested. If the Trust cannot comply with the request the reason(s) will be documented and the individual will be advised of these in writing, where possible.

7.4 This information will be provided free of charge. However, if a request is deemed to be manifestly unfounded or excessive, in particular because of their repetitive character, a reasonable fee may be charged or the request may be refused.

8 Access to Disclosure of Images to Third Parties

8.1 Disclosure of recorded material to third parties will be considered in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of crime
- Prosecution agencies
- Relevant legal representatives
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings
- Emergency services and other authorised agencies in connection with the investigation of an accident.

8.2 The third party requiring the recorded image must complete a Data Subject Access Request Form (see Appendix 5) which must be submitted to the Data Protection Officer for consideration and possible release of recorded image(s).

9 Retention of Images

9.1 The Data Protection Act does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. The Trust's standard retention period of recorded images is 28 days from the point of recording unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

9.2 All images on electronic storage will be erased by automated system overwriting. Any downloads, still photographs and hard copy prints will be securely disposed of as confidential waste. The date and method of destruction will be recorded on the original Data Subject Access Request Form, if applicable, held by Data Protection Officer.

10 Monitoring Compliance

10.1 All staff involved in the operation of the Trust's CCTV system will be made aware of this policy and an annually procedure will be required for staff to read and acknowledge the policy.

10.2 All staff with responsibility for accessing, recording, disclosing, or otherwise processing CCTV images will be required to undertake data protection training.

11 Complaints Regarding the Operation of the CCTV System

11.1 Complaints regarding the CCTV system and its operation should be made using the Trust Complaints Procedure.

12. Policy Breach

12.1 Failure to comply with this Policy may lead to disciplinary and potentially legal action.

13 Forms for use with this Policy

- Request Record of Viewing CCTV Data Form or electronic form (Appendix 3)
- Request to Carry Out Covert CCTV Recording (Appendix 4)
- Data Subject Access Request Form (Appendix 5)

14 Review of Policy

14.1 The Closed Circuit Television (CCTV) Policy and Procedure will be reviewed in line with future legislative changes, case law or at no later than 3 years after the issue date.

14.2 The planned review date for the Data Protection Policy and Procedure is August 2027

APPENDIX 1 Data Protection Impact Assessment

Follow the link below for a template to conduct a data protection impact assessments.

Data Protection Impact Assessments for surveillance cameras

APPENDIX 2 Authorised Postholders

(Names of specific individuals authorised within this list are held by the Data Protection Officer)

POST HOLDER
Trust CEO
Chief Finance Officer
Schools Heads and Senior Leadership Team
Data Protection Officer
Head of Operations
Head of Estates
School Premises Managers
Authorised Appointed Agents
IT and authorised contractors maintaining the CCTV system.

APPENDIX 3 Request for Record of Viewing CCTV Data Form

REQUEST RECORD OF VIEWING CCTV DATA FORM

School
Name of Person Viewing Data
Reason for viewing CCTV Data (ie Safeguarding, Criminal act etc)
In an emergency or time critical situation - please provide details for retrospectively authorisation so an assessment can be completed of that requirement by the DPO.
Incident Date/Time and brief description of required incident:
Requested by (Name/Position/Warrant Card Number/photo ID):
Signature of Person Requesting: …… **Date: ……**
Signature of Authoriser: …… Data Protection Officer **Date: ……**
Reason for refusal of request:
Signed: …….. Data Protection Officer **Date: ……...**

APPENDIX 4 Request to Carry Out Covert CCTV Recording

REQUEST TO CARRY OUT COVERT CCTV RECORDING

To: Data Protection Officer
Date Requested: …….
Reason for request:
Location for covert CCTV:
Length of time covert CCTV required:
Requested by (Name and Position):
Signature of Person Requesting: …… **Date: ……..**
Authorised by: …… CEO / CFO
Signature of Authoriser: …… **Date: ……**
Reason for refusal of request:
Signed: …….. CEO / CFO **Date: ……...**

APPENDIX 5 Data Subject Access Request Form

Data Subject Access Request Form - CCTV

1. Your details

Title:	Mr	☐	Mrs	☐	Miss	☐	Ms	☐	Other ☐
Forename(s)									
Surname									
Date of birth									
Current address									
Home phone									
Mobile									
Email address									

Current student ☐ Previous student ☐ 3rd Party ☐

Current employee ☐ Previous employee ☐ Police ☐

Other (please state) _____

2. Request being made as:

3. Proof of Identify

We require proof of your identity before we can respond to your access request. To help us establish your identity, please provide identification that clearly shows your name, date of birth ***and*** current address. We can accept a photocopy or a scanned image of one of the following:

- Passport
- Photo identification such as a driver's licence, national identification number, birth or adoption certificate.
- Student identification
- Warrant card

Please also attach a copy of a bank statement, credit card statement or utility bill showing your current address and must be dated within the last **three months**. (Unless you are a member of staff of Bridgwater and Taunton Trust, law enforcement or legal profession.)

Please note, we may request additional information from you to help confirm your identity. We reserve the right to refuse to act on your request if we are unable to identify you.

4. Details of your request:

Please describe the information you seek together with any other relevant information to help us identify the information you require (such as relating to a specific course or period of time). Please provide the reason for the request (please continue on a separate sheet if necessary).

If requesting CCTV images, please make sure you have included:

- date and time the images were recorded;
- information to identify the individual, if necessary; and
- location

5. Fee

We reserve the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information. The fee is based on the administrative cost of providing the information.

6. Declaration

I certify that the information provide on this form is true and correct.

Full name _____

Signature _____ Date _____

Please return the completed form to: Data Protection Officer, Bridgwater and Taunton College Trust, Parkway, Bridgwater, Somerset TA6 or email to dataprotection@btc-trust.org

We will respond to your request within 30 days, where we are unable to approve your request for information or unable to provide the information within 30 days, we will notify you.

FOR TRUST USE ONLY				
Identification document				
Request approved	Yes / No	Reason for refusal		
Request approved by				
Format of data provided				
Signed:			Date:	
Date and method of destruction (if applicable)				
Signed:			Date:	