TRINITY SCHOOL
CARLISLE

A CHURCH OF ENGLAND ACADEMY

CCTV (CLOSE CIRCUIT TELEVISION) AND VIEWING PROCEDURE

Full Governing Body
Reviewed: March 2024
Ratified by the Governing Body: March 2024
Next review: March 2026

Contents

Data Protection Statement

Any personal data processed in the delivery of this policy will be processed following the UK GDPR and the Data Protection Act (2018) and under the School's Data Protection Policy and Procedures.

1. Policy Statement

1.1 Trinity School uses Close Circuit Television ("CCTV") within and around the School. The purpose of this policy is to set out the position of the in relation to its management, operation and use of CCTV and should be read inconjunction with the School's *Data Protection Policy*.

1.2 This policy applies to all members of our school community including staff, students, governors and visitors, and all other persons whose images may be captured by the CCTV system while on School premises.

1.3 This policy takes account of all applicable legislation and guidance, including:

- United Kingdom General Data Protection Regulation ("UK GDPR");
- Data Protection Act (2018)
- CCTV Code of Practice produced by the Information Commissioner;
- Human Rights Act 1998.

1.4 The system comprises several internal and external fixed and dome cameras. The system does not use any sound recording capability. The CCTV system is owned and operated by the School and the deployment of CCTV is determined by the Senior Leadership Team. The Headteacher or their designated alternative has overall responsibility as delegated by the Board of Governors.

1.5 The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018.

1.6 Access and viewing are restricted (refer to section 9 below). All authorised operators with access to images are aware of the procedures they are required to follow and their responsibilities under this policy.

1.7 All employees will be aware of the restrictions concerning access to, and disclosure of, recorded images.

1.8 Changes to, or the introduction of a new CCTV system will be subject to consultation with relevant stakeholder where appropriate, and a Data Protection Impact Assessment will be undertaken before any changes are made.

2. Purpose of CCTV

2.1 The School uses CCTV for the following purposes:

- to increase the personal safety of students, employees and visitors, reduce the fear of crime and encourage good student behaviour;
- to protect the School buildings and their assets;
- to support the Police in a bid to deter and detect crime;
- to assist in identifying, apprehending and potentially prosecuting offenders;
- to protect members of the public and private property;
- to assist in the safeguarding of students in and around the site.

2.2 If in the event of viewing CCTV for a specified purpose, the CCTV can and may be used for a disciplinary investigation.

3. Policy Intent

3.1 The School will:

- notify the Information Commissioners Office of its use of CCTV as part of the annual data protection registration;
- complete a CCTV Privacy Impact Assessment ("PIA") for the use of surveillance CCTV and update this as appropriate when the system is upgraded or significantly modified;
- treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act and the UK GDPR;
- not direct cameras outside of the School site at private property, an individual, their property or a specific group of individuals. The exception to this would be where authorisation was obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000;
- display CCTV warning signs which will be clearly and prominently placed at all external entrances of the School site where CCTV is operational, including the School gates as coverage includes outdoor areas. The School will ensure that there are prominent signs placed at the entrance of the CCTV zone and within the controlled area. Signage will contain details of the purpose for using CCTV.
- not guarantee that a system will or can cover or detect every single incident taking place in the areas of coverage;
- not use materials or knowledge for any commercial purpose. Recorded materials will only be released for use in the investigation of a specific crime with specific safeguards under the authority of a competent authority and in compliance with the Data Protection Act 2018 and the UK GDPR.

4. Siting Cameras

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. For example, cameras will not be placed in areas that are reasonably expected to be private such as intoilets or changing rooms. The School will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the requirements of the Data Protection Legislation.

4.2 CCTV is not routinely sited in classrooms, except in the Zone, and will not be used in such, except in exceptional circumstances;

- to increase the personal safety of students, employees and visitors, reduce the fear of crime and encourage good student behaviour;
- to assist in the safeguarding of students in and around the site.

4.3 Members of staff, on request, may access details of CCTV camera locations.

5. Data Storage, Retention and Security

5.1 Camera surveillance will be maintained at all times. Footage will be continuously recorded and held on the system memory for a maximum of 30 days except where the image identifies an issue and is retained specifically in the context of an investigation and/or prosecution of that issue.

5.2 Where data is required to support an investigation and/or/prosecution the data is saved to an electronic file held on a secure central server with restricted access.

5.3 To maintain and preserve the integrity of any recordings of events extracted from the hard drive and the facility to retrieve them for use in any future proceedings, each recording must be identified by a unique file name and recorded in the CCTV Log.

5.4 The Data Protection Act (2018) does not prescribe any specific minimum or maximum retention periods for CCTV systems or footage. The retention period for these files will be reflected by the School's purposes for extraction, and they will be deleted as soon as that purpose is achieved.

5.5 Access to recordings is outlined in section 7, below

6. Access to CCTV Images

6.1 Access for Internal Use

- CCTV recorded images may be viewed by authorised members of the School for supervisory and investigatory purposes, disciplinary reasons or authorised demonstration and training. CCTV data used within the School's discipline and grievance procedures will be subject to the usual confidentiality requirements of those procedures. In those circumstances, disclosure of CCTV recordings may be made to service providers where these would reasonably require access to the data (e.g. HR, Trade Unions, Insurance Providers).

- The ability to view live and historical CCTV data available via network software is only to be provided to authorised persons. Direct access to recorded data is limited to the I.T. team (as administrators), the Headteacher, SLT, Heads of Year, the Premises Managers, and members of the pastoral team.

- Specific live monitoring is provided to <<insert relevant staff/locations e.g, Reception, Sixth Form Leadership Team and Sports Hall staff>> for live footage of restricted cameras.

- Data from CCTV may be used within the School's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

- At times, other staff may request to view CCTV images will be made via email detailing the legitimate reason for viewing and authorised by the Headteacher or, in their absence, a designated Senior Member of staff acting on their behalf.

- Recorded images will be made available to staff who have direct involvement in investigating a reported incident on receipt of an authorised email.

- Members of staff who have witnessed or been involved in, an incident may be asked to review images to identify individuals or to establish facts about the incident.

- The viewing of CCTV images will be recorded in the CCTV Log and referenced to the accompanying authorisation email.

- Authorised viewing of CCTV recordings will be limited to individuals on a need-to-know basis.

6.2 Access and Disclosure of Images to Police or other Competent Authorities

- Recordings may be viewed by the Police or other 'competent authority' as defined in section 30 of the Data Protection Act 2018, for the "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security", under section 29 of the Data Protection Act 2018.

- Viewing of CCTV images by the Police must be requested using the CCTV Viewing request: Police and Other Competent Authority form. Once access has been provided, this should be recorded in the viewing log and the Access form stored appropriately. Access to CCTV by competent authorities must be managed by the Headteacher or a delegated alternative.

- The Police may require the School to retain CCTV data for possible use as evidence in the future. Such disk(s) will be properly indexed and securely stored under the management of the Headteacher or their designated alternative.

- Should a recording be required as evidence, a copy may be released to the Police under the procedures described below:

- A recording required for evidential purposes will be provided in pairs on identical media with each carrying an identical identification number. The Master recording is to be retained securely by the School in a sealed bag. The other copy may be released to the police or another authorised third- party (Police Officers, Special Constabulary or CID staff, or other competent authority) on the production of:

    - an ***Access Request Form*** signed by an officer with a rank **no lower than** Police Inspector.

    - Picture Identification for the receiving officer such as Police Warrant Card, Picture ID Card, Driving Licence, etc.

- The receiving authority will become the data controller in respect of any personal data that is provided to them and must adhere to all data protection legislation in their handling of that personal data

- On occasions when a Court requires the release of an original recording stored by the School, this will be retrieved from secure storage and presented in its original sealed bag.

- If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice should be sought if necessary.

- Applications received from external bodies (e.g. solicitors) to view or release footage will be referred to the Data Protection Officer. In these circumstances, recordings will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, or in response to a Court Order.

6.3 Disclosure of Images to Data Subjects (Subject Access Requests)

- Any Individual recorded in any CCTV image is a data subject under the Data Protection Legislation and has the right to request access to those images.
- Any individual who requests access to images of themselves will be considered to have made a Subject Access Request under the Data Protection Legislation. Such a request should be considered and managed in the context of the School's 'Subject Access Request Policy and Procedure'.
- The School must accept a Subject Access request made in any form – written or verbal, including via its social media channels, and to any member of staff. Individuals submitting requests for access will be asked to provide sufficient information (e.g., date, time, location) to enable the footage relating to them to be identified.
- When such a request is made a member of staff with authorised access will review the CCTV footage, to determine whether the footage contains images of the requester, or not.
- If the footage contains images of the individual making the request then the individual may be permitted to view the footage. Viewing must be strictly limited to that footage that contains images of the requester within the parameters of the request. The I.T Team as the CCTV system administrators must take appropriate measures to ensure that the footage is restricted in this way.
- If the footage contains images of other individuals, then the School must consider whether:
    - The request requires the disclosure of the images of individuals other than the requester, for example, whether the images can be distorted so as not to identify other individuals;
    - The consent of other individuals in the footage could be obtained; or
    - If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- The School reserves the right to refuse access to CCTV footage where this would prejudice the rights of other individuals or jeopardise an ongoing investigation.

6.4 Recording CCTV Access

- A record must be kept, and held securely, of all internal and external requests to view CCTV images. Copies of Viewing Request Forms and Logs are included in Appendix A-D below.

7. Complaints

7.1 Complaints and enquiries about the operation of CCTV within the School should be directed to the Headteacher in the first instance.

8. Further Information

8.1 For further information on CCTV and Data Protection please see:

- Data Protection Act (2018)
- United Kingdon General Data Protection Regulations (UK GDPR)

- CCTV Code of Practice

9. Monitoring and Review

9.1 The Headteacher, together with the Data Protection Officer, are responsible for monitoring and reviewing this policy.

9.2 This Policy will be reviewed and updated as and when necessary in response to any amendments to Data Protection Legislation, or any concerns arising from policy violations, data breaches, or on an annual basis.

Appendix A: Police and Competent Authorities Viewing Form

Viewing of CCTV Images Form: Police or Other Competent Authority

Reference No: POCA/

(Format: POCA/next no. in viewing log)

This form must be completed before the viewing of CCTV images to the Police or other competent authority as defined in section 30 of the Data Protection Act 2018.

Name of Requester								
Rank (if applicable)								
Enforcement Agency (✓)	Police		Special Constabulary		CID			
Other: (insert detail)								
Confirmation of ID: (✓)	Warrant card		Picture ID		Driving Licence			
	Other:							

I make formal application for access to view/listen to and (if necessary) request a copy CCTV recorded data of an occurrence/incident within the School site which occurred:

On (date): _____ At (time): _____

Viewing Authorised by:

Name:			
Position:		**Date:**	
Date of viewing		**Facilitated by:**	

Potential Evidence: Data Extraction, Retention & Release

The viewed data is to be:	**x**
Extracted and retained by the School	
Extracted and released to the authority on production of a completed Access Request Form	

The Police or other competent authority may require the School to retain CCTV data for possible use as evidence in the future. The data will be properly indexed and securely stored under the management of the Headteacher or their designated alternative.

Data extracted by:		**Date:**	
Storage Media used:		**Recording ID No.**	
Storage location:			

Data Extraction & Release

CCTV Data required for evidential purposes will be provided in pairs on identical media with each carrying an identical identification number. The Master recording is to be retained securely by the School in a sealed bag. The other copy may be released to the police or another competent authority as defined in section 30 of the Data Protection Act 2018 on the production of an Access Request form signed by an officer with a rank no lower than Police Inspector.

Data extracted by: (2 copies)		**Date:**	
Media used:		**Recording ID No.**	
Master sealed by:			
Storage location:			
Access Form Received	Yes/No	**Checked by**	
Data Copy received by:			
Signature:		**Date:**	

Notes:

Appendix B: Request for disclosure of information under Schedule 2 Part 1(2) of the Data Protection Act (2018)

Organisations that have a crime prevention, law enforcement or tax collection function may require personal information held at Trinity School to prevent or detect a crime, or apprehend or prosecute an offender, or for taxation purposes.

The following form must be completed before Trinity School will consider any request for information under Schedule 2 Part 1(2) of the Data Protection Act (2018). For more information, please refer to the Guidance Document below.

All requests must be submitted either in person, via secure email or by registered post. Please note that fax is not considered a secure method of transmission.

Recipient authorities will become the data controller in respect of any personal data that is disclosed to them under this request and must adhere to all data protection legislation in your handling of that personal data.

Section 1 – Requester Details

Requested by (name in full)	
Organisation	
Job Title	
Address	
Telephone number	
Email address	
Your reference	
Date of request	

Section 2 – Legal Gateway

(a) The prevention or detection of crime	☐
(b) The apprehension or prosecution of offenders	☐
(c) Assessment or collection of tax, duty or imposition of similar nature	☐

Please list which conditions of Article 6 and Article 9 of the General Data Protection Regulation that you are relying on to support your application for the disclosure of information. See GDPR: Lawfulness of processing below

Section 3 – Data Subject Details

Name	
Address	
Other identifying information	

Specific Information Required	

Section 4 – Information to support disclosure

Alleged Offence(s)	
Reason Information is necessary	
State under which statutory powers you are requesting the information	

Section 5 – Authorisation

I can confirm that the personal data requested are required for the purpose(s) stated above and failure to provide information will, in my view, be likely to prejudice that/those purpose(s).

Name (please print)				
Organisation		Rank		
Signature			Date	

Police Request Only

This request must also be authorised by a person no lower than Police Inspector.

Name (please print)				
Organisation		Rank		
Signature			Date	

Request for disclosure of information under Schedule 2 Part 1(2) the Data Protection Act (2018): Guidance

Introduction
Organisations that have crime prevention, law enforcement or tax collection function may require personal information held by Trinity School to prevent or detect a crime, or apprehend or prosecute an offender, or for taxation/benefit purposes.

Examples of organisations that can submit requests under Schedule 2 Part 1(2) are; Police, HM Revenue and Customs, other Local Authorities or Public Bodies, acting under authorised Powers

Trinity School may be able to release this information by application of an exemption under Schedule 2 Part 1(2) of the Data Protection Act 2018. There is no obligation on the School to do so and even if the exemptions apply the School may decide that it should not release any information.

Please note that if the School has genuine concerns about releasing any personal information (for example, because it thinks it has other legal obligations such as the information being confidential) then we may ask for a court order requiring the release of the information.

How to make a request under Schedule 2 Part 1(2) of the DPA (2018)
To make it easier for the Police and other competent authorities requesting information under Schedule 2 Part 1(2) of the Act, Trinity School has created a form that should be completed before a request will be considered. Requests can be submitted either via secure email, by registered post, in person

Contact details

Postal Address: Trinity School, Strand Road, Carlisle. CA1 1JB

Email – info@trinity.cumbria.sch.uk

Data Protection Officer: The Schools People, 44 Tyndall Court, Peterborough, PE2 6LR

Email: DPOservice@schoolspeople.co.uk

Failure to complete the form fully is likely to delay the process of obtaining the information.

GDPR: Lawfulness of processing

Article 6: Processing general category data

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

    a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

    b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.

    c) processing is necessary for compliance with a legal obligation to which the controller is subject.

    d) processing is necessary to protect the vital interests of the data subject or another natural person.

    e) processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.

    f) processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Article 9: Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

    a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

    b) processing is necessary for carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

    c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

    d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

    e) the processing relates to personal data which are manifestly made public by the data subject.

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) processing is necessary for reasons of substantial public interest, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) processing is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on domestic law or under contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and medicinal products or medical devices, based on domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under Article 89(1) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix C: CCTV Viewing Log

CCTV: Viewing Log

			Request Form		Police/Competent Authority: Retention and Release of Data			
Reference	**Date of Viewing**	**Category of Viewer**	**Reference No:**	**Hyper-Link to Request Form**	**Data Retained**	**Data Released**	**ID Number**	**Storage Location**
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								