CCTV Policy

Data Protection Officer | September 2026

Minsthorpe
Community College

Contents

	Page
1. Introduction	2
2. Purpose of the Policy	2
3. Scope	3
4. General Principles	3
5. Justification for use of CCTV	4
6. Location of Cameras	4
7. Notification – Signage	5
8. Storage & Retention	6
9. Access	6
10. Responsibilities – The Principal's will:	7
APPENDIX 1 – DEFINITIONS	8
APPENDIX 2 - PRIVACY IMPACT ASSESSMENT	9
Final Section	12

- Equality Assessment
- Updates
- Policy Review Schedule

1.
Section 1

Introduction

Closed Circuit Television Systems (CCTVS) are installed at Minsthorpe Community College in key areas.

Section 2

Purpose of the Policy

The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring the premises of Minsthorpe Community College.

CCTV surveillance at the Minsthorpe is intended for the purposes of:

- enhancing security of the building and its associated equipment.
- protecting the school buildings and College assets, both during and after College hours;
- promoting the health and safety of staff, pupils and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the College rules are respected so that the College can be properly managed.

Section 3

Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out, the College will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

Section 4

General Principals

Minsthorpe has a statutory responsibility for the protection of its property, equipment as well providing a sense of security to its employees, students and invitees to its premises.

Minsthorpe owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the College community by integrating the best practices governing the public and private surveillance of its premises.

The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Information obtained through the CCTV system may only be released when authorised by the Principals. The college will share CCTV footage with the Police should this be required.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies including Anti bullying Policy, Staff Handbook, Equality Policy, Behaviour Policy, Code of Conduct, Data Protection Policy, Sexual Harassment Policy and other relevant policies.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

CCTV monitoring of public areas for security purposes within College premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

All CCTV systems and associated equipment will be required to be compliant with this policy.

Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Acts 1988 and 2003.

Section 5

Justification for use of CCTV

Section 2(1)(c)(iii) of the Data Protection Acts requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the College needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the perimeter of the College buildings for security purposes has been deemed to be justified by the Leadership Team.

In other areas of the College where CCTV has been installed, the Principal has demonstrated that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

Section 6

Location of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify, the College has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

Section 7

Notification - Signage

The Principal will provide a copy of this CCTV Policy on request to staff, students, parents and visitors to the College. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Leadership Team. Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the College.



WARNING
CCTV cameras in operation
Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of Minsthorpe Academy Trust and its property. This system will be in operation 24 hours a day, every day. These images may be passed to the Police.
This scheme is controlled by Minsthorpe Academy Trust
For more information contact *01977 657600*.....

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, school gates,
- reception area,
- at or close to each internal camera.

Section 8

Storage & Retention

Section 2(1)(c)(iv) of the Data Protection Acts states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue — such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

Accordingly, the images captured by the CCTV system will be retained for a maximum of 1 week, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Principal. The Principal may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Police, Assistant Principals, the relevant Year Head, other members of the teaching staff. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to know basis.

Section 9

Access

The recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Principal.

In relevant circumstances, CCTV footage may be accessed by:

Subject Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. The College will not release any footage where other individuals (who are not included in the SAR) can be identified. To exercise their right of access, a data subject must make an application in writing.

Individuals will be invited to College to view any footage, however if the image is of such poor quality as not to clearly identify an individual, the request will not be fulfilled.

Individuals (or their legal representatives) subject to a court order.

The Police where Minsthorpe (or its agents) are required by law to make a report regarding the commission of a suspected crime; or

Following a request by the Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Minsthorpe's property, or

Requests by the Police: Information obtained through video monitoring will only be released when authorised by the Principal. If the Police request CCTV images for a specific investigation, the Police may require a warrant and accordingly any such request made by the Police should be made in writing, Minsthorpe should immediately seek legal advice.

The HSE and/or any other statutory body charged with child safeguarding.

The Principal in establishing facts in cases of unacceptable student behaviour.

An Insurance company where the insurance company requires to pursue a claim for damage done to the insured property.

A person should provide all the necessary information to assist Minsthorpe in locating the CCTV recorded data, such as the date, time and location of the recording.

Section 10

Responsibilities – The Principal's will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by Minsthorpe Community College
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within Minsthorpe Community College
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring at Minsthorpe Community College is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system
- Ensure that monitoring recorded tapes are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally

- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the College and be mindful that no such infringement is likely to take place
- Co-operate with the Health & Safety Officer of Minsthorpe Community College in reporting on the CCTV system in operation in the College
- That adequate signage at appropriate and prominent locations is displayed as detailed above
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 1 week and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- Ensure that where the Police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Principal.

APPENDIX 1 – DEFINITIONS

- Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;
- CCTV — Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.
- The Data Protection Acts — The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All College staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation
- Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).
- Personal Data — Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
- Subject Access Request —this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.
- Data Processing - performing any operation or set of operations on data, including:
    - Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
    - Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available, Aligning, combining, blocking, erasing or destroying the data.
- Data Subject — an individual who is the subject of personal data.
- Data Controller - a person who (either alone or with others) controls the contents and use of personal data.
- Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

APPENDIX 2 - PRIVACY IMPACT ASSESSMENT

- Before a College/School installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. A College/School which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against the College by the Office of the Data Protection Commissioner, or may expose the College to a claim for damages from a student.
- Some of the points that might be included in a Privacy Impact Assessment are:
- What is the College's purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?
- Are the CCTV cameras intended to operate on the outside of the premises only?
- Is it justified under the circumstances?
- Is it proportionate to the problem it is designed to deal with?
- Is it intended that CCTV cameras will operate inside of the building?
- Are internal CCTV cameras justified under the circumstances?
- Are internal CCTV cameras proportionate to the problem they are designed to deal with?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the College need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Will the system being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed? Is the College, the data controller for the entire CCTV system (bearing in mind that some schools under the PPP are managed for operational purposes by management companies, in which case specific legal advice may need to be sought)?.
- Where a management company is in place, is the College satisfied that it complies with the Data Protection Acts with regard to the processing of images of staff, students and visitors to your school captured on any CCTV systems under its management?
- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, students and visitors been assured by the School that they will not be monitored and that the CCTV system will be used only for the stated purposes?
- Does the College's policy on the use of CCTV make it clear that staff (teaching and nonteaching) will not be monitored for performance or conduct purposes?
- Have the views of staff & students regarding the location of cameras been taken into account?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been erected at the location of each internal camera indicating that recording is taking place and outlining the purpose of such recording?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images? Are those who will have authorised access to the system and recordings/images clear about their responsibilities?

- Are the camera monitors kept out of view of staff, students and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis? Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does the College have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (28 days) has expired?
- Does the College have a procedure in place for handling requests for access to recordings/images from the Police?
- Will appropriate notices be in place to ensure that individuals know that they are being monitored?
- Does the College have a data protection policy? Has is been updated to take account of the introduction of a CCTV system?
- Does the College have a procedure in place to handle access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of forty days)?
- Has the right of access been communicated to staff, students and visitors?
- Has the College communicated its policy on the use of CCTV to staff, students and visitors and how has this been done?
- How are new students and new staff informed of the school's policy on the use of CCTV?

Final Section

Equality Assessment

This policy has been assessed with regard to its impact on equalities issue, with specific reference to the aims of the Equality Act 2010. The equality impact assessment focused on race, gender, disability, pregnancy and maternity, age, sexual orientation, gender reassignment and religion/belief.

Updates

Sept 26 – minor updates

Policy Review Schedule

Policy last reviewed:	Due for next review:	Role Responsible:
September 2022	September 2024	Data Protection Officer
September 2024	September 2026	Data Protection Officer