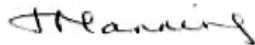






## CCTV and Body Worn Camera Policy

**Policy Ref: TMP90v1**

This policy will not discriminate either directly or indirectly against any individual on grounds of sex, race, ethnicity or national origin, gender, sexual orientation, marital status, religion or belief, age, disability, socioeconomic status, offending background or any other personal characteristic.

	Name	Title	Signature	Date
Prepared by	Jackie Manning	Principal		Sep 2025
	Colin Foster	Assistant Principal		Sep 2025
Approved by	Martin Heaton	CEO		Sep 2025

Does this Policy require publishing on the College Website? Yes

Does this Policy require approval by Board of Governors? Yes

# CCTV and Body Worn Camera Policy

Policy Ref: 90v1

## Record of Changes

Version	Issue Date	Changes	Initials
v1	Sep 2025	Initial issue	JM/CF

**Date of Next Policy Review:** July 2026

## Definitions

Throughout this policy document **TMP Studios CIC** is referred to as 'TMP College'.

*Surveillance* – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.

*Body Worn Camera (BWC)* – Portable devices that record audio and video

*CCTV – Closed-Circuit Television* - a surveillance system that sends video signals to a limited number of screens or recording devices. The system may or may not also include audio signals.

## Scope

TMP College is committed to maximising its effectiveness in tackling antisocial behaviour, reducing crime and disorder and maintaining a safe and secure environment for staff, students and members of the public whilst on College property.

In support of this aim, we use surveillance cameras and Body Worn Cameras (BWC's) to protect staff and the students, discourage aggressive and abusive behaviour and provide evidence where required to investigate complaints.

This policy sets out the purpose of using BWC's, what information will be recorded, who will have access to this information and how this information will be stored and disposed of.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at TMP College and ensure that:

- We comply with the UK GDPR.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

BWC'S's and CCTV will not be used in the ad-hoc monitoring of staff.

We will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any toilet or changing facility.

We notify all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, signs, letters and emails.

If the surveillance and CCTV systems fulfil their purpose and are no longer required, we will deactivate them.

## Key Principles

*Non-Discrimination:* The use of BWCs and CCTV will be implemented in a manner that does not discriminate against any individual or group. All staff and students will be treated with respect and dignity.

*Inclusivity:* This policy is designed to be inclusive, ensuring that the needs and rights of all individuals, including those from protected characteristic groups, are considered and respected.

*Transparency:* Clear information about the use of BWCs and CCTV, including the purpose, data storage, and access rights, will be communicated to all stakeholders. This ensures transparency and builds trust within the college community.

*Accountability:* Regular monitoring and evaluation of the BWC Policy will be conducted to ensure compliance with equality legislation and to address any potential negative impacts on specific groups.

## Aims

TMP's surveillance at the College is intended for the following purposes:

- Reduce and deter crime and disorder
- Reduce and deter anti-social behaviour
- Provide a safe and secure environment
- Reduce potential escalation of incidents
- Capture images close up, including audio recording
- Help to protect staff at work (for health and safety purposes)
- Provide evidence to support internal and when required external investigations (police)
- Assist in the investigation of allegations of inappropriate conduct by staff

## BWC Operating Procedure

All BWC operators will receive training in the use of BWC, including: -

- Practical use of equipment
- Operational guidance i.e. when to commence and cease recording
- Legal implications of using such equipment.

The day-to-day management of the BWC system will be the responsibility of the designated member of staff for that system.

BWC will be activated for recording when the operator: -

- Has an engagement with a member of the public, staff or student which, in the opinion of the operator, is confrontational and where they believe that they may be subject to physical or verbal abuse

- Encounter a situation in which they are approached by a member of the public, staff or student in a manner perceived as aggressive or threatening

BWC will only be used by staff when wearing College uniform or clearly displaying College identification. BWC will not be used in a hidden or covert manner.

In all instances where BWC are to be used, and where practical, operators will inform the individual (or group) that the BWC is switched on and recording. This will ensure that both the maximum deterrent value is achieved and that the public are fully aware that they are being recorded.

If questioned, the operator must confirm to the enquirer that they are subject to recording and be prepared to answer questions as to the security of the data.

There may be occasions when informing an individual would escalate the incident or put the operator in danger if such a warning was given, but this should be very rare and the operator may be required to justify such an action.

We respect and support the individual's entitlement to go about their lawful business and this is a primary consideration in the operation of a BWC system. Although there is inevitably some loss of privacy when BWC's are operational, cameras will not be used to monitor the progress of individuals in the ordinary course of lawful business in the area under surveillance.

Individuals will only be continuously monitored if there is reasonable cause to suspect an offence or serious breach of discipline has been, or may be, about to be committed.

### **Retention of BWC and CCTV recordings**

Any recordings which have been made will be uploaded and stored on TMP College's secure IT network. All data is backed up and stored for 35 days. After a period of 35 days, all recordings will be permanently deleted.

BWC recordings will only be retained for longer than 35 days in instances where an investigation or disciplinary case has not concluded.

BWC recordings may only be accessed by TMP College's Security Manager, Senior Leadership Team, Designated Safeguarding Leads, or other senior staff involved in investigations. Any other staff requiring access to the data must be authorised by the one of these groups through the SLT.

BWC recordings will be made accessible as soon as practicable to the Police upon its request.

If a member of the public has been identified as being recorded by BWC, he / she can request to view the recording. The request will be treated as a subject access request under Section 7 data Protection Act 2018.

Availability of the BWC recordings will be subject to the retention period described above.

All footage will be in the form of a still, unless a legal requirement states a video is needed. This is to the personal information of people who may be in the background of the recording.

Other legal body's may request footage in line with the data information request procedure.

### **Data protection principles**

TMP College understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The surveillance and CCTV system is owned by TMP College and images from the system are strictly controlled and monitored by authorised personnel only.

We notify all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, signs, letters and emails.

Data collected from surveillance and CCTV will be:

- Processed lawfully,
- Processed fairly, in a manner that people would reasonably expect and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified, and legitimate purposes and not further processed in a manner that is incompatible with the following purposes; further processing for archiving data in the public interest, scientific or historical research purposes or statistical purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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, using appropriate technical or organisational measures

Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

The surveillance system will be registered with the ICO in line with data protection legislation.

Warning signs must be placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

The surveillance system has been designed for maximum effectiveness and efficiency; however, we cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be used to focus on a particular group unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the College.

## **Access**

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All disks and hard drives containing images belong to and remain the property of TMP College.

Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for
- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.
- Certain research activities.
- Compliance with a specific legal obligation.

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the College or they object to way it was processed.

Data can be restricted by either:

- Moving the data to another processing system.
- Making the data unavailable to users
- Temporarily removing published data from a website.

TMP College will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

we may impose a 'reasonable fee' to comply with requests for further copies of the same information. The individual will either be provided with a permanent copy of the information or allowed to view the information.

Requests by persons outside the College for viewing or copying surveillance recordings will be assessed by the Principal, on a case-by-case basis, with close regard to data protection and freedom of information legislation.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the College holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the College will ask the individual to specify the information the request is in relation to.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent, or removing specific footage where appropriate.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the 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
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded and the Principal will make the final decision as to whether recorded images may be released to persons other than the police.



## **Security**

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected, and where appropriate, will be encrypted.

Staff will be trained in security procedures and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

## **Appendix 1**

### **Legal Framework and Guidance**

This policy has due regard to all relevant legislation and statutory guidance, including, but not limited to the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'
- DfE (2022) 'Protection of biometric data of children in schools and colleges'