Richmond upon Thames College

2021-22

Policy Name:	CCTV Policy
Policy Number/Version No:	Version 3
Effective Date:	March 2022
Review Date:	May 2023
Policy Responsibility:	Data Protection Officer
Approved By:	Audit Committee / Corporation
For Action By:	All
For Information to:	Head of Estates and Facilities

Version Control:

CONTENTS **PAGE**

1. INTRODUCTION

Richmond upon Thames College (RuTC) is fully committed to operating a safe environment, it therefore has in place a closed-circuit television ("CCTV") system to assist in providing a safe and secure environment for students, staff, and visitors, as well as protecting the College's property.

in addition to the use of CCTV the college also deploys Body Worn Cameras ("BWC") worn by the security team to record video, stills and sound recordings of incidents as a means of gathering evidence of violence, threats etc…

Further detail is available in the Body worn Cameras (BWC) Privacy Impact Assessment, Appendix C.

CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act 2018. The person ultimately responsible for data protection within the College is the College Principal.

The system comprises several fixed and dome cameras located both internally and externally around the College site. All cameras maybe monitored and are only available for use by approved members of staff.

The CCTV system is owned by RuTC and will be subject to review on an annual basis.

The purpose of this Policy is to regulate the management, operation, and use of the CCTV system at the College. This document sets out the accepted use and management of the CCTV system and images to ensure the College complies with the Data Protection Act 2018, Human Rights Act 1998, and other legislation.

The College has produced this policy in line with the Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

2. PURPOSE OF CCTV

2.1 The College has installed CCTV systems to:

- Protect College buildings and other assets to ensure they are kept free from intrusion, vandalism, damage, or disruption
- To increase the personal safety of staff and students and reduce the fear of physical abuse, intimidation, and crime.
- To support the Police in a bid to deter and detect crime.
- Assist in prevention and detection of crime.
- Assist with the identification, apprehension, and prosecution of offenders.
- Assist with the identification of actions/activities that might result in disciplinary proceedings against staff and students.
- Assist in the usage and management of the College buildings on a day-to-day basis.
- Provide management information relating to Contract Compliance of 3rd party service providers.
- Monitor security of campus buildings.
- Identify vehicle movement problems around the campus.

The system will be provided and operated in a way that is consistent with an individual's right to privacy.

2.2 Covert Recording

Prior to authorisation the requesting applicant must have demonstrated and documented that all reasonable procedures and practices were put in place to prevent suspected illegal or unauthorised activity from taking place.

Any such covert processing will only be carried out for a limited and reasonable period consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom. The Colleges Legal Team may be involved in approving and assessing the need for covert recording in all instances.

Covert cameras may be used under the following circumstances on the written or electronic authorisation of the Principal or another member of SLT acting as their deputy, as appropriate.

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording.

- That there is reasonable cause to suspect that illegal activity is taking place or is about to take place or unauthorised activity is taking place; that may seriously or substantially affect the operation or reputation of the College.

Unless required for evidential purposes or the investigation of crime or otherwise required by law, covertly recorded images will be retained for no longer than 31 days from the date of recording. A record of data destruction will be made in confirmation on the authorised request to make covert recordings.

The system will not be used to:

- Provide images to the world wide web
- Record sound
- Disclose to the media

3. Operation

The CCTV surveillance system is owned by the College.

The Head of Estates is responsible for the operation of the system and ensuring compliance with this policy. This day-to-day role will be delegated to the Contract site Security Supervisor who will hold an SIA CCTV Licence.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both Data Protection Act 2018 and the Commissioner's Code of Practice.

Cameras will be used to monitor activities within the College buildings, car parks and other areas to identify criminal activity occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the occupants within the College grounds, together with its visitors.

Static cameras will not focus on private homes, gardens, and other areas of private property.

When operating cameras with tilt and pan and zoom capacity, users will not direct cameras at an individual, their property or a specific group of individuals, without verbal authorisation from the Head of Estates or deputy holding a SIA CCTV Licence unless an immediate response to events is required.

Materials or knowledge secured in connection with the CCTV system will not be used for any commercial purpose. Downloads will only be released to the media for use in the investigation of a specific crime and with written authority of the Police. Downloads will never be released to the media for the purposes of entertainment.

The planning and design of the CCTV system has endeavoured to ensure that it will give maximum effectiveness and efficiently but is not possible to guarantee that it will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes and areas covered by the CCTV System.

Image Viewing and Download Procedure

- Recordings may be viewed by the Police and authorised officers.
- Permission to do this will be given as follows by:
    - Head of Estates and Facilities – Student, visitors / public incidents
    - Principal or Deputy Principal – Staff incidents
- Should a download be required as evidence, an electronic copy may only be made by a holder of a SIA CCTV licence.
- Where this is to be released to the Police this will only be on receipt of a Data Release Form and sight of their warrant card.
- Where this is requested by the Principal and Deputy Principal a CCTV Request Form will be completed and given to the Head of Estates and Facilities.
- Where this is requested by a member of SLT / Duty Officer/ Investigating Officer investigating into a student incident a CCTV Request Form will be completed and given to the Head of Estates.

3.1 Breaches of this Policy

Any suspected breach of this Policy by College Staff will be considered under the College`s Disciplinary Policy and Procedures.

4. <u>Overview of System</u>

The CCTV system runs 24 hours a day, 7 days a week but images are not monitored throughout this period.

The CCTV system comprises 15 fixed position cameras, monitors and public information screens.

CCTV cameras are located at strategics points on in the main building, principally at the entrance and exit points of the building as well as main thoroughfares outside toilets on every level.

CCTV signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors, and members of the public that a CCTV installation is in use and its purpose.

Although every effort has been made to ensure maximum effectiveness of the CCTV system; it does not cover all areas and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

5. Data Protection Act

For the purpose of the Data Protection Act 2018 the College is the data controller.

- CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act 2018. This policy is associated with the College's Data Protection Policy, the provisions of which should be always adhered to.
- The College has registered its processing of personal data (including CCTV) with the Information Commissioners Office (ICO).

Where new cameras are to be installed on college premises, part 4 of the ICO`s CCTV Code of practice will be followed before installation:

- The appropriateness of and reasons for using CCTV will be assessed and documented.
- The purpose of the proposed CCTV system will be established and documented.
- Responsibility for day-to-day compliance with this policy will be established and documented.

6. Access to Images

6.1 Individual Access Rights

The Data Protection Act 2018 gives individuals the right to access personal information about themselves, including CCTV images.

All requests for access to view/ copy CCTV footage by individuals should be made in writing to the Head of Estates and Facilities.

Requests for access to CCTV images must include:

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

The College will respond promptly and at the latest within the 30 calendar days of the receiving the request processing fee, determined by the head of Estates and Facilities and sufficient information to identify the images requested.

If the College cannot comply with the request, the reasons will be documented.
The requester will be advised of these in writing, where possible.

6.2 Access to Images by Third Parties

Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e., images not of the person making the request) do not have a right of access to images under the DPA, and care must be taken when complying with such requests to ensure that neither the DPA, HRA or the CCTV Policy are breached. As noted above, requests from third parties will only be granted if the requester satisfies the following criteria:

- Law Enforcement Agencies (where the images recorded would assist in a specific criminal enquiry)
- Prosecution Agencies and their Legal Representatives
- Insurance Companies and their Legal Representatives

All third-party requests for access to a copy of CCTV footage should be made in writing to the Head of Estates and Facilities.

A law enforcement or prosecution agency is requesting access they should make a request under Section 29 of the Data Protection Act 1998.

7. Retention and Disposal

Recorded images will be retained for no longer than 31 days from the date of recording, unless required for evidential purposes or the investigation of a crime or otherwise required and retained as a download with the requisite approval form.

All images on electronic storage will be erased by automated system overwriting. All 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 bottom of the original approval to copy held by the Head of Estates and Facilities.

8. Central Responsibilities

The Vice Principal, Finance and Planning (as Data Protection Officer) is responsible for producing and reviewing this Policy.

The College Leadership Team is responsible for approving this Policy.

The Head of Estates and Facilities is responsible for compliance with and implementation of procedures to comply with this policy.

9. Complaints regarding operation of system

Complaints regarding the CCTV system and its operation should be made under the College complaints procedure.

10. Associated Policies and Guidance

CCTV Code of Practice
Home Office Surveillance Camera Code of Practice.

11. Forms for Use with this Policy

- Request to carry out Covert Recording
- Data Release Form (Police)
- Data Release Form (HR)
- Data release Form (Head of Estates & College Investigating Officers / Student Incidents)

Appendix A

Richmond upon Thames College

Request to carry out Covert Recording

To: Head of Estates and Facilities	
Authorised by: (Principal/Deputy Principal)	
Reason for request: (Incident Ref No. if relevant)	
Location, date, and time required:	
Length of time required:	
Date requested:	
Requested by:	
Signature:	
Position:	

Head of Estates and Facilities to confirm data has been disposed of	
Date:	
Method of destruction:	
Signed:	
Print name:	
Date:	
Additional Comments/ Notes	

Appendix B

Richmond upon Thames College

CCTV/ BWC Release Form

Name:
Date:

Please provide brief description of the CCTV/ BWC footage including the date, time and location covered.

Released by:

I accept that the footage is supplied to me without prejudice. I understand that it was recorded on private premises and includes third parties. In accordance with the Data Protection Act 2018 and in compliance with regulations laid down by the Information Commissioner, I will not publish, broadcast, undermine due confidence, nor otherwise cause any breach of the personal data, nor further process the data in a manner where it could affect the rights and freedoms of any other individual or groups of individuals. I understand that all relevant parties reserve the right to protection of the law and any breach could result in legal proceedings.

Signed:	Date:

Appendix C

Body-Worn Video (BWV) Privacy Impact Assessment

Richmond Upon Thames College Security Staff carry body worn video cameras (BWV). The cameras are always worn overtly by uniformed staff during deployment. This equipment has been introduced in many Colleges and Local Authorities to deter and detect crime and anti-social behaviour.

The cameras will not ordinarily be turned on and will only be activated when the officer is responding to an incident where it is deemed necessary, and any activation will be announced. The use of these cameras is in accordance with the following documents and legislation.

- RuTC (Richmond upon Thames College) CCTV Policy
- The Information Commissioners PIA codes of practice
- The Surveillance Camera Commissioners Principles and best practice.

This Privacy Impact Assessment has been written to cover issues in the use of BWV and to explain:

- The rationale for College Security using this technology
- The legality behind its use
- The operational circumstances when security officers may use BWV
- Key privacy issues/risks and an explanation of mitigation measures in place

BWV is proven to cause a reduction in incidents and supports the CCTV systems that will act as a principal deterrent to reduce any conflicts and de-escalate incidents to safeguard our students and staff.

There are key objectives for their activation by the security team. They are not continually recording and will only be activated for recording when justified, such as by being alerted to an incident occurring.

The principal purpose of deployment is as follows:

to obtain evidence of an incident that is indisputable as to behaviour /conduct witnessed that may be against our student conduct codes, or criminal behaviour that poses health and safety risks to students, the College, or its staff.

a) To act as deterrent and prevention to escalation of misconduct or criminal conduct

b) To protect the security team and staff including duty officers in proving fair conduct in dealing with any incident. This includes having to ever demonstrate the use of reasonable and proportionate force / restraint when legally required within Education Act guidelines

c) To use the BWV as recording evidence of any incident outside the College's grounds, such as in the alleyway, Harlequin's car park, the Craneford Way Playing Fields area, or surroundings that we can legally record in a public place to provide to Police of a crime, incident, or safety issue, if necessary, that impacts on safety and security of the College, students, or staff. This would include the recording of students, or any other person captured for obtaining evidence of a crime or major incident

d) To warn the subject that their activity may legally be captured and recorded for use in disciplinary hearings or criminal investigation so that they are aware that evidence captured is legally obtained.

Purpose of Privacy Impact Assessment (PIA) Any project or set of new processes that involve exchanging personal information has the potentialt to raise privacy concerns from the public. This document is a method by which to alleviate any public concerns for the use of this new recent technology.

The Information Commissioner's Office Code of Practice recommends the application of 'screening questions' to confirm or otherwise the requirement for a Privacy Impact Assessment and to indicate its appropriate scale and detail. These questions are re-produced in the table below:

No.	Question	Response
1	Does the project apply new or additional information technologies that have the potential to invade the privacy of any individuals and/ or employees?	BWV is an established technology being utilised by the College's Security Team. This technology is only ever deployed in an overt manner, using trained uniformed staff and in defined operational circumstances. All captured data is processed to ensure compliance with Regulation 2016/6791 (GDPR (General Data Protection Regulations), the Data Protection Act and the Human Rights Act 1998, the Information Commissioners Code of Practice, and the Surveillance Camera Commissioners guidance.
2	Does the project hold sensitive information that could potentially expose the identity of the individuals and/ or employees and require new security measures?	Yes. BWV holds personal data requiring appropriate network and hardware security.
3	Does the project have the capacity to continue without identifying any of the individuals and/ or employees?	No. Only identified employees have access to the BWV camera software. No unidentified employee has access to this software. It is the purpose of BWV that subjects be capable of identification.
4	Does the project involve working with multiple organisations, whether they are government agencies or private sector organisations (e.g., as outsourced service providers or as 'business partners')?	When capturing information on these devices, staff only do so to fulfil a lawful purpose. The legitimate purpose behind the use of this equipment is to prevent and detect crime and prevent public disorder. When information is captured, it is assessed as to

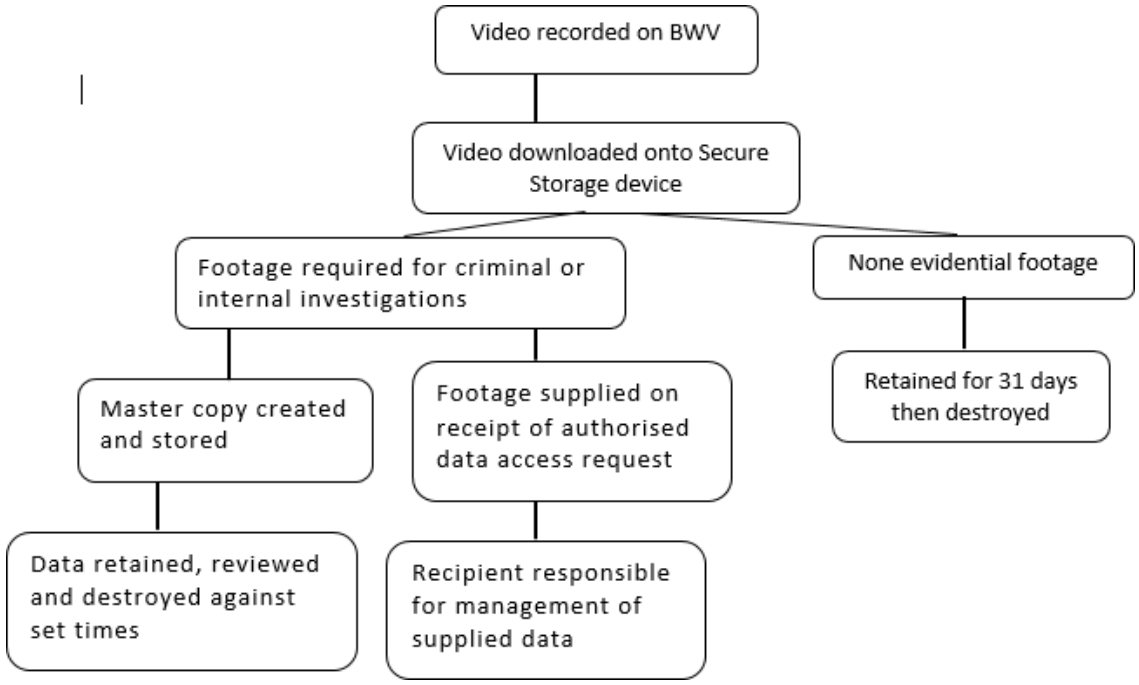
		whether it constitutes evidential or non-evidential material. Any material which is deemed as evidential could then be shared with the Police and other prosecuting agencies and to managers undertaking internal investigations. There are occasions when BWV material could be shared with other agencies to assist in training and to support a multi-agency approach to any legitimate, justified working arrangement.The BWV and the software used supplies data in a format suitable for sharing with those agencies that may request the data.
5	Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals and/ or employees?	No. There is no change to the handling of personal data compared to current usage. Images of people whether victims, suspected offenders, witnesses, bystanders, or officers are captured on BWV before being stored securely, like existing CCTV protocols.
6	Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual and/ or employees in the database requiring new retention arrangements?	No. The project generates relatively small amounts of data. The retention arrangements are the same as for CCTV and the new software allows for automatic deletion of non-evidential footage after a set period (which can be amended by administrators).
7	Does the project involve new or significantly altered handling of personal data about a substantial number many individuals and/ or employees?	No. Numbers of individuals concerned will be small and data will be automatically deleted as per the existing retention policy for video data.
8	Does the project involve new or significantly changed consolidation, inter-linking, cross- referencing, or matching of personal data from multiple sources?	No. Although it is possible that investigations could involve the creation of composite video evidence e.g., bringing together BWV and CCTV or other forms of digital evidence, there is no routine or systemised means of doing so.
9	Does the project relate to data processing which is in any way exempt from legislative privacy protections e.g. The Data Protection Act/GDPR?	Richmond Upon Thames College only deploys this technology against the defined operational requirements and to ensure that the use is proportionate, legitimate, necessary, and in addition, it will ensure that the use satisfies the requirement of addressing a pressing social need. At all stages it will comply with Regulation 2016/6791 (GDPR (General Data Protection Regulations), the Data Protection Act and other legislation. In the case of the Human Rights Act 1998, there is adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home, and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier.

10	Does the project's justification include significant contributions to public security?	Yes. Included in the social need for the prevention and detection of crime, is a public safety and security of both staff and students at the college.
11	Will the project be the subject of consultation both internally and externally?	Yes. The project is already under consultation internally.

1. The Information Flows

The Security Team has the responsibility for the processing of information in its possession which commences at the point when an officer captures it.

BWV operational guidelines are given to all staff who are issued BWV devices, it informsstaff when it is appropriate to use them/what to say and how information is captured on a BWV device is then used, captured, processed, and disposed of.



In circumstances where the information is evidential, master or working copies are created and retained.

At the end of any investigation, there is a requirement to hold the data strictly in accordance with the Data Protection Act and GDPR (General Data Protection Regulations) requirements, which includes undertaking reviews, retention extensions if appropriate and then secure disposal.

Where information is passed to law enforcement agencies, those agencies take on the responsibility for the retention management and disposal of that information.

All other material will be automatically erased after 31 days. Access to recordings will be controlled and only People who have an operational need to view specific incidents may do so.

The master copy remains as a digital file in the storage device. The storage device is a Richmond Upon Thames College managed server that IT (Information Technology) services have created and limited access to. This is a copy of the original recording, which is stored securely, pending its production (if required) at court or at a college hearing / Tribunal.

A working copy (the version produced from the original media for the investigation) of this is then made available after being burnt on to a DVD. All video captured will be managed in accordance with relevant legislation and the College's CCTV code of practice.

2. The general privacy and related risks of surveillance technology

The usage of BWV does not record all activity on a continuous basis. Doing so would significantly impact on the privacy of the public, who are going about their normal lives, as well as the privacy of staff going about their duties. Such a practice would require the storing, reviewing and then disposal of large quantities of personal data.

BWV is currently used as a means of capturing key evidence in such a way that it can bring a compelling and accurate account of the circumstances at that time. This does not replace the need to use other types of evidence but does go a considerable way in reducing any ambiguities and should be considered as an additional security aid.

The equipment is worn by uniformed Security staff and the use is primarily driven by the incidents and circumstances presented to them or in anticipation of responding to a reported and unfolding incident. The camera recording will only be activated when it is both reasonable and necessary to do so based on this risk assessment.

To activate the record function requires the officer to deliberately activate the device to a record mode and where practicable, make a verbal announcement to indicate that the BWV equipment has been activated. This announcement should be present on the recording and if possible, should include:

- The nature of the incident to which the user is deployed.
- Confirmation to those present that the incident is now being recordedusing both video and audio.

If the recording has commenced prior to their arrival at the scene of an incident the officer should, as soon as is practicable, declare to those people present that recording is taking place and that their actions and sounds are being recorded. Announcements should be made using simple terminology that can be easily understood by those present.

The pre-recorded footage will help clarify reasoning for the activation of the BWV by showing any escalation of events leading up to an incident.

The technology being introduced includes an LED (Light Emitting Diode) light to alert users and others that a recording has started.

Once the record switch is used, the s LED (Light Emitting Diode) changes colour and it is then recording mode. Unless specific circumstances dictate otherwise, recording must continue uninterrupted from the moment it starts until the conclusion of the incident or the resumption of general patrolling.

At the conclusion of any incident, the recording on the device is switched off and the captured information is stored.

The recording is also likely to continue for a short period after the incident to clearly demonstrate to any subsequent viewer that the incident has concluded, and that the user has resumed other duties or activities.

Where practicable, users should make an announcement that the recording is about to finish. Prior to concluding recording, the user should make a verbal announcement to indicate the reason for ending the recording. This should state the reason for concluding the recording.

3. The privacy and related risks of BWV

Privacy Issue	Risk to Individuals	Compliance Risk	College risk
Collection of data	Contravention of privacy rights Unauthorised access to data	Regulation 2016/6791(GDPR (General Data Protection Regulations), - contravenes Principle 1 (Lawfulness,fairness, and transparency)	Regulation 2016/6791 (GDPR (General Data Protection Regulations) comprises seven principles and data controllers have a legal obligation to comply with these principles. The data subject must be informed of the identity of the data controller; the purpose or purposes for which the material is intended to be processed; and any further information that is necessary for processing to be fair. The data controller is the Interim Vice Principal for Finance and Planning, Richmond Upon Thames College Data losses which damage individuals could lead to claims for compensation.
Loss or misuse of data	A failure to account for a full audit trail Footage being kept for longer than necessary	Regulation 2016/6791 (GDPR (General Data Protection Regulations), - contravenes Principle 6 (Integrity and confidentiality, security)	
Footage being recorded unnecessarily	If a retention period is not established information might be used for longer than necessary.	Regulation 2016/6791 (GDPR (General Data Protection Regulations), - contravenes Principle 3 (Data minimization)	The data will be stored on a Richmond Upon Thames College managed server, with access granted only to employees who have had specific training, permitted on authority of a Security Manager. BWV cameras will not always record, and any footage will be deleted after 31 days if not being retained for authorised investigatory purposes.
Recorded images (in private areas as opposed to public areas)	Misuse of footage	Human Rights Act 1998 – contravenes Article 8 (the right to respect for private and family life, home, and correspondence)	The use by security staff of BWV must be shown to be proportionate, legitimate, necessary, and justifiable. In addition, use of the equipment should address a 'pressing social need' especially in respect of its application within the confines of the Articles enshrined by the European Convention of Human Rights

			(incorporated into the Human Rights Act 1998).
The potential for covert surveillance	Contravention of privacy rights		Security surveillance activities in respect of BWV will be overt. BWV devices will not be used in a covert manner. Security will ensure the use of BWV is highly visible to the public and the officer wearing the equipment will announce its use.

4. Solutions to the Privacy Risks

Risk	Solution
Collection/ use / loss of data	Access to data only available to Security Team Managers. Persons entitled to access data identified in CCTV Code of Practice. All data signed for by person receiving the data.
Footage being recorded unnecessarily	The system has been set up to retain data for the correct retention period (maximum 31 days before deletion).
Recorded images (in privateas opposed to public areas)	Any attempt to delete any recording whilst on duty will be clearly identified (via the audit trail) once the camera is returned to the Estates Office. There will also be a log of the individually assigned cameras, which shows the user who was assigned the BWV camera.
The use of images in court proceedings	All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, practical use e.g.,when to commence and cease recording, and health and safety.
The potential for covert surveillance	BWV will only be deployed in an overt manner.

5. Evaluation of the Solutions to the Privacy Risks

What are the safeguards for minimising the retention times for data?

Any information captured on a device, which is deemed to be non-evidential, will be automatically deleted after a set period (31 days). The rationale for any retention beyond an immediate disposal might include circumstances where there is a desire to review any allegations as part of the College's complaints procedure, the reporting of these more often occurring the aftermath of any incident and often this material may not have been marked as evidential. Other data within the evidential category will be retained to satisfy the requirements of legislation, the court process if applicable and depending on the type of offence retained, reviewed, and disposed of, in accordance with timeframes within the Data Protection Act.

What are the procedures for dealing with the loss of any BWV devices?

Users are instructed that BWV devices should be held securely when not being worn. When not in

use they will be placed in their docking station, located within the access-controlled Estate Manager's Office.

Due to the nature of Security patrolling, it is possible such as within a public order or violent encounter that a device might be lost and fall into the hands of unauthorised persons. Where a device is lost, all attempts will be made to identify and notify people who are subject of information on the device. The University of Warwick will also report the loss at the earliest opportunity.

In response the following safeguards have been put in place; -

- Security adopts a process whereby the devices are assigned to individual officers. The officers are responsible for reporting any loss immediately. Accordingly, the impact in terms of any time lost between any actual loss and notification of the College is kept to a minimum.
- The data held on the device is protected in both the software and hardware as such data cannot be accessed from the device itself.
- When the device is connected to the secure storage device and software any data is automatically downloaded onto it, and then deleted from the device. The software itself is also encrypted and can only be accessed by authorised persons using their username and password.
- Access to stored data is restricted, audited and dependent on an individual's role.

How will collateral intrusion be handled?

Collateral intrusion in this context extends to the capturing of the movements and actions of other people when this equipment is being used.

It is inevitable that in some circumstances this will occur, albeit staff are trained to ensure that wherever possible, the focus of their activity is on the person subject to the officer's attention.

In circumstances where unrelated persons are captured in any video or audio information their identities will be protected and anonymised especially should the matter be presented in proceedings.

The introduction of new software allows this to be completed more easily and can be configured to anonymise both images and audio.

Do you need consent to record an individual?

No. There is no requirement to obtain the consent of the person or persons being filmed since the actions of the user are deemed to be lawful. If someone requests that the BWV be switched off, the security officer should advise the person that:

- Any non-evidential material is only retained for a maximum of 31 days
- This material is restricted and cannot be disclosed to third parties without express authority of the subject of the recording unless prescribed by law; and
- Recorded material is the College's information and it can be accessed on request to the Data Protection Officer in writing in accordance with the GDPR (General Data Protection Regulations) unless an exemption applies in the circumstances.

Security Officers will consider on a case-by-case basis whether to switch the BWV device off. There should always be a presumption to record if the 'need to address a pressing social need' has been achieved unless the circumstances dictate otherwise. An officer failing to record an incident may be required to justify the actions as vigorously as any officer who chooses to record a like encounter.
Recording can only be justified when it is relevant to the incident and required to gather evidence.

Audio Recording is a greater infringement of privacy, how can this be justified?

BWV is seen to have major benefits of capturing evidence in an indisputable fashion. To ensure that all aspects of an incident are captured, this requires the essential inclusion of audio information for this to be complementary to the video data.

The other important aspect of the addition of audio information is that in some instances, the camera itself may not be pointing in the direction of the main incident but that the audio will still be captured.

This has a significant advantage of protecting all parties to ensure that the actions of security staff were totally in accordance with the law and addresses issues of transparency. Equally, in some instances, the presence of only video evidence without the added context of audio, can fail to provide the full context, for all parties, of an incident or interaction.

6. Review of the Privacy Impact Assessment

The system used will be regularly tested to ensure its efficiency in protecting the footage captured. Procedures will be regularly checked to ensure the best practices are followed, to identify problems in the procedures and to amend / update them, as necessary.

Estates will review the impact of BWV cameras annually.

Please refer to RUTC CCTV Policy and CCTV/BWC Privacy Impact Assessment

CCTV only to be retrieved by Security Supervisor or Head of Estates

Richmond upon Thames College

Staff able to authorise CCTV capture

Jason Jones Principal

Mark Brough Head of Estates, Facilities & Security

Michael Clifford Student Liaison Manager

Authorisation for CCTV/ BWC footage

Date	Time	Request from	CCTV/BWV Operator	Reason for request	Authorisation given	Authorised Manager	Date/ Time
					YES / NO		
					YES / NO		
					YES / NO		
					YES / NO		
					YES / NO		
					YES / NO		
					YES / NO		
					YES / NO		