Wiltshire College
& University Centre

Closed Circuit Television

Document administration

Document version:	2.2
Date of formal issue:	23 May 2024
Document reference:	EF_POL_001
Document type:	Policy
Document owner:	Head of Estates & Services
Date of next review:	23 May 2027
Person responsible for review:	Finance and Maintenance Manager

Amendment log

Ver	Date	Reason for amendment	Name
1.0	01/0615	Initial issue	NK
2.0	05/01/23	Review and major update	Gerry Fordham
2.1	23/05/24	Review and sent for approval	Andy Hill
2.2	26/06/24	Approved with minor comments	SLT

Approvals

Document prepared by:	**Full name:**	Gerry Fordham
	Role:	Finance and Maintenance Manager
	Date:	05 Jan 2023

Reviewed by:	**Full name:**	Andy Hill
	Role:	Head of Estates
	Date:	23 May 2024

Authorised for publication by:	**Full name:**	Steve Campion
	Role:	Deputy Principal, Corporate Resources
	Date:	26 June 2024
	Signature:	

Table of contents

Glossary

Item	Description
CCTV	Closed Circuit Television.
DPA	Data Protection Act 1998.
FOI	Freedom of Information.
GDPR	General Data Protection Regulations.
ICO	Information Commissioner's Office.
NK	Not known.
PDF	Portable Document Format.
SAR	Subject Access Request.
H&S	Health & Safety
SLT	Senior Leadership Team.
SOP	Standard Operating Procedure.

1. Introduction

1.1. Wiltshire College & University Centre, referred to as 'the College' for the remainder of this document, is fully committed to providing a safe environment.

1.2. In response to a suitable and sufficient security risk assessment being carried out, it has identified and agreed that Closed-Circuit Television (CCTV) is a reasonable control measure.

1.3. The College has installed private CCTV systems on all sites to assist in providing a safe and secure environment for employees, students, contractors and visitors, as well as protecting college property.

2. Purpose

2.1. The purpose of this policy is to regulate the management, operation and use of the CCTV system used by the College. The primary aim of the CCTV system is to:

2.1.1. Increase the personal safety of employees and students and reduce the fear of physical abuse, intimidation, and crime.

2.1.2. Protect college buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption.

2.1.3. Support law enforcement in a bid to deter and detect crime.

2.1.4. Assist with the identification of actions / activities that might result in disciplinary proceedings against employees and students.

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

3. Scope

3.1. This policy shall cover the following groups of people:

3.1.1. Employees.

3.1.2. Students.

3.1.3. Contractors.

3.1.4. Visitors.

3.2. This policy shall cover the following sites:

3.2.1. Castle Combe Centre.

3.2.2. Chippenham Campus.

3.2.3. Corsham Centre.

3.2.4. Lackham Campus.

3.2.5. Salisbury Campus.

3.2.6. Trowbridge Campus.

3.3. This policy shall cover routine working hours and outside of college hours, including weekends and holidays. Extended services shall also be included.

3.4. This policy shall not include any premises either owned or managed by the Castle Combe Racing Circuit.

3.5. This policy shall not cover any activity conducted at a location / site other than those listed above.

4. Definitions

Closed Circuit Television

4.1. Also known as video surveillance, is the use of video cameras to capture and transmit images through a private network, to recorders and monitors, primarily for the purposes of surveillance and security.

CCTV System

4.2. Any hardware, firmware, software, lighting or installation equipment used in the capture of any digital media.

Direct Access to CCTV

4.3 Means access to the CCTV systems, the cameras and any information stored within them

In-direct Access to CCTV

4.4 Means access to view Digital Media, either within the CCTV system and viewed on a screen or Media that has been downloaded and stored outside of the CCTV system.

5. Digital media

5.1. Any communication media, such as image or video, that operate with the use of any of various encoded machine-readable data formats. Digital media can be created, viewed, distributed, modified, listened to, and preserved on a digital electronics device.

Controller

5.2. The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor

5.3. ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Employees of the controller are not processors. As long as they are acting within the scope of their duties as an employee, they are acting as an agent of the controller itself. They are part of the controller, not a separate party contracted to process data on the controller’s behalf.

Subject access request

5.4. Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a Subject Access Request (SAR). A third party can also make a SAR on behalf of another person (with their written agreement).

Public CCTV

5.5. Public CCTV would be that which you find on streets, car parks, highways, parks etc. As these areas are deemed public, the police are able to access the footage filmed in these spaces. It is unlikely to be in real-time, it is more likely to be a download of a recording. There is no Public CCTV in the College.

Private CCTV

5.6. Private CCTV footage would be classified as anything on privately owned land such as a home, small business premises, pubs etc. If, however, cameras happen to catch footage on areas such as pavements then that would classify as public meaning the rules are slightly different. This footage would need to comply with the Data Protection Act / requirements of GDPR.

6. Responsibilities

Principal

6.1. The Principal shall:

6.1.1. Be responsible and accountable for policy performance.

6.1.2. Ensure that adequate funding and resources are allocated to enhance college security.

Deputy Principle Corporate Resources

6.2. The Deputy Principal for Corporate Resources shall:

6.2.1. Monitor the implementation of this policy.

6.2.2. Ensure that all risks associated with CCTV are assessed and effectively controlled.

6.2.3. Appoint a competent person to act as Data Controller.

Head of Estates & Services

6.3. The Head of Estates & Services shall:

6.3.1. Act as the Data Controller.

6.3.2. Implement effective policies & procedures to control the installation, operation, servicing and maintenance of any equipment and/or software associated with college surveillance.

6.3.3. Authorise all third-party requests for access to any digital media.

6.3.4. Investigate and manage any incidents of non-compliance and/or breaches.

6.4. Estates Finance and Maintenance Manager

6.4.1. The estates Finance and Maintenance Manager shall deputise for the Head of Estates and Services in all duties set out in Para 5.3.

Data Controller

6.5. The Controller shall:

6.5.1. Exercise overall control of the personal data being processed and be ultimately in charge of and responsible for the processing.

6.5.2. Ensure that CCTV is identified as a control measure within the risk assessment for security and emergency planning.

6.5.3. Control the release of data to the media for use in the investigation of a specific crime, once authorised by the Police.

6.5.4. Comply with UK GDPR.

Site Manager

6.6. The Site Manager shall:

6.6.1. Be responsible for the day-to-day operation of the CCTV system on their campus, ensuring compliance with this policy.

6.6.2. Ensure that CCTV is considered within a suitable and sufficient risk assessment.

6.6.3. Ensure the CCTV system is installed, serviced, and maintained by a competent person, with records kept.

6.6.4. Restrict access to all viewing monitors, recording equipment and digital media.

6.6.5. Strictly control the release of any digital media relevant to the authorised SAR.

6.6.6. Ensure that all digital media is disposed of in accordance with this policy.

CCTV Operator

6.7. The CCTV Operator shall:

6.7.1. Respect the privacy of any individuals and/or neighbouring properties outside the scope of this policy.

6.7.2. Follow the training received when using this system.

6.7.3. Tell someone if they think the work or inadequate precautions are putting anyone's health and safety at serious risk.

All employees

6.8. All employees shall:

6.8.1. Comply with this policy to ensure the safety of all employees, students, contractors and visitors.

6.8.2. Not modify or interfere with any CCTV installations.

6.8.3. Tell someone if they have a suspicion or concern relating to college security.

7. System overview

7.1. The CCTV system shall operate 24 hours a day, seven days a week and will be managed and maintained by the relevant Site Manager.

7.2. The system comprises of:

7.2.1. Fixed position cameras.

7.2.2. Pan, tilt and zoom cameras.

7.2.3. Monitors.

7.2.4. Multiplexers.

7.2.5. Digital recorders.

7.2.6. Public information signs.

7.3. Body worn cameras are not used within the College and may not be used without written approval from the Principal.

7.4. Every effort shall be made to ensure maximum effectiveness of the CCTV system, however, it shall 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.

8. Data Control

8.1. For the purpose of UK GDPR, the Head of Estates & Services shall act as the designated Data Controller.

8.2. Digital media, such as CCTV digital images, that show a recognisable person, are considered to be personal data and covered by UK GDPR.

8.3. Where applicable, the College shall register its processing of personal data (including CCTV) with the ICO.

8.4. Where new cameras are to be installed on college premises, the ICO CCTV Code of Practice shall be followed before installation. This shall include:

8.4.1. The appropriateness of and reasons for using CCTV will be assessed and documented.

8.4.2. The purpose of the proposed CCTV system will be established and documented.

8.4.3. Responsibility for day-to-day compliance with this policy will be established and documented.

9. CCTV system

9.1. The CCTV system is owned by the College and its implementation as a control measure will be subject to review on an annual basis.

9.2. The CCTV systems comprise of a number of fixed and movable cameras located both internally and externally around each site.

9.3. The CCTV system is not turned off – it operates every day, including when the College is closed.

9.4. Care shall be taken to ensure that the CCTV system only covers college premises and those public areas and entrances around student residential accommodation.

10. Access to CCTV Systems.

10.1. Direct Access to the CCTV system will only be granted to approved persons approved by the Data Control or his Deputy. Direct Access will include (but is not necessarily limited to):

10.1.1. Head of Estates and Services

Estates Finance and Maintenance Manager

Estates Site Managers

Estates Site Officers

Education Security Officers

Learning Resource Centre staff

Residential Accommodation Staff.

Such IT staff as are required for the management fo the CCTV system.

10.2. Direct Access to the CCTV systems is granted in two ways:

10.2.1. For the Avigilon system, through College IT accounts (single user login). The IT Department is to ensure that access to this system is granted only to authorised persons.

10.2.2. For legacy IT systems, through password controlled accounts on individual DVRs. These passwords are to be closely controlled and not given to un-authorised persons.

10.3. Indirect Access to CCTV

10.4. Viewing of media within the CCTV system or that have been downloaded / stored outside of the CCTV system will be managed by the relevant Campus Manager in accordance with the Estates CCTV Standard Operating Procedure (SOP)/

11. Procurement

11.1. All CCTV hardware & software shall be purchased by a competent person from an approved supplier, ensuring that security, updates, quality, maintenance, disposal and the environment is a primary consideration.

11.2. Equipment shall be accompanied with the manufacturer's instructions and any technical specifications.

11.3. Digital media produced by the CCTV system shall be as clear as possible so that they are effective for the purposes for which they are intended.

12. Security

12.1. The College shall ensure that any CCTV equipment and/or services provided adheres to the highest security protocols considered to be reasonable for the given circumstances.

12.2. Hardware used for the recording and viewing of images shall be stored in a secure location with controlled access.

12.3. Software used for the storage and viewing of images shall be protected from uncontrolled access (internal and external).

12.4. Access to any CCTV hardware for recording shall be protected from theft and/or interference at all times whilst the building is unoccupied.

12.5. Approved storage devices used for the transfer of data shall be adequately protected from unauthorised viewing. Such devices shall not be taken off site without permission from the Data Controller.

12.6. Digital media (and associated data) shall not be stored on any personal devices, such as laptops, mobile phones and USB memory sticks.

13. Privacy

13.1. Static cameras shall not be directed at:

13.1.1. Student accommodation windows.

13.1.2. Private homes & gardens.

13.1.3. Other areas of private property.

13.2. CCTV operators of cameras with tilt and pan and zoom capability shall not direct cameras at an individual, their property, or a specific group of individuals, without verbal authorisation from the Site Manager (or their deputy) unless an immediate response to an incident is required.

13.3. Privacy shall be a key consideration when operating the CCTV system.

14. Copyright

14.1. Wiltshire College & University Centre shall own, and retain, the copyright on any images created by the CCTV system.

15. Cameras

15.1. Live monitoring is permitted only within the Learning Resource Centres and the Lackham Residential Accommodation. Outside of those areas, cameras shall not be routinely live monitored.

15.2. Cameras shall be located at strategic points on site, principally at the entrance and exit point(s) and around various buildings, as well as main thoroughfares and common areas throughout the site.

15.3. All cameras shall be allocated a unique reference number that is easily read at the point of installation. This reference shall be used when processing any requests for information.

16. Lighting

16.1. Adequate lighting shall be installed internally and externally to support the effective capturing of viewable images.

16.2. Lighting equipment shall be selected and positioned in a way so as to avoid disturbing neighbouring properties.

16.3. The use of intelligent lighting, such as infrared, should be used, where possible, to minimise any unnecessary light pollution.

17. Signage

17.1. Appropriate CCTV warning signs shall be prominently placed at strategic points and at entrance and exit points of the site to inform employees, students, contractors, visitors and members of the public that a CCTV installation is in use, its purpose and details of the operator.

17.2. Signage shall be checked at regular intervals by Site Managers to ensure that they remain clean and effective.

18. Operation

18.1. The CCTV system shall be operated by a competent person in accordance with the manufacturer's instructions.

18.2. CCTV operators shall receive written Standard Operating Procedures (SOP) for all key activities / tasks relating to their role.

19. Maintenance

19.1. All CCTV equipment shall be installed, serviced and maintained, in accordance with the manufacturer's instructions, by a competent person, with records kept.

19.2. Maintenance shall also include adequate testing and inspections to identify any unauthorised modifications of the system.

19.3. All CCTV firmware and software shall be checked at regular intervals to ensure that the latest versions are installed.

20. Digital Media management

20.1. In the event of an incident requiring Digital Media to be stored, Authorised Persons may record the Media within the CCTV system.

20.2. The media (and associated data) shall be reviewed for the purpose of identifying 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.

20.3. All data shall be protected so it is not accessible by any unauthorised personnel

20.4. Images may only be shared (including viewing on a screen) with non-authorised persons by an Estates Site Manager, the Head of Estates or the Estates Finance and Maintenance Manager. To protect the data, this must be done in accordance with the Estates CCTV SOP – so one of the above must be contacted in the event the CCTV Media is required to be shared.

20.5. The Site Manager or authorised Deputy may take action to download and save Media that may relate to an incident involving employees or others until such time that it has been decided that it is required for viewing and/or download or it can be erased.

20.6. Media that may be required as evidence may only be downloaded and saved made by the Site Manager (or one of those approved in para 19.4).

20.7. All digital media, once downloaded, shall be adequately protected to prevent unauthorised viewing.

20.8. All requests to obtain a copy of any Digital Media (and associated data) created by the CCTV system shall be submitted to the Exams and Compliance Manager using a Subject Access Request (SAR) form.

20.9. SOPs shall be created to control access to all private digital media from employees and any outside interested parties, such as the Police, legal representatives or insurers.

20.10. Digital media shall only be released to the Police on receipt of formal documentation.

21. Subject Access Requests

21.1. All request for Data made for reasons other than College business (i.e insurance request for staff or students, external requests) will be treated as Subject Access Requests. The College shall respond to a SAR within one month of receipt of the request. This time may be extended by a further two months if the request is complex or a number of requests have been received from the same individual.

21.2. Requests to access digital media (and associated data) created by this CCTV system shall include the following information (as a minimum):

21.2.1. The reason for the request.

21.2.2. The date and time the images were recorded.

21.2.3. Information to identify the individual, if necessary.

21.2.4. The location of the CCTV camera.

21.2.5. Proof of Identity.

21.3. The College shall perform a reasonable search for the requested information and will provide the information in an accessible, concise and intelligible format.

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

21.5. The information shall be delivered to the individual securely (password protected).

21.6. The College may refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

21.7. The College shall plan to cover two forms of delivery in response to an approved SAR:

21.7.1. Online access, viewing the CCTV hardware (monitor).

21.7.2. Offline access, viewing a downloaded or printed copy.

21.8. The College shall plan to cover requests for digital media (and associated data) from:

21.8.1. Employee requesting data relating to a student incident.

21.8.2. Employee requesting data relating to an employee incident.

21.8.3. Request from law enforcement.

21.8.4. Request from an official representative.

21.8.5. Request from the individual affected.

21.8.6. Media.

21.8.7. Other parties.

Employee requesting data relating to a student incident.

21.9. Digital media (and associated data) relating to a student incident may be saved by the Site Manager but is only to be shared with Head of Department / Deputy Head of Department who are not to save copies.

21.10. For student related incidents, the Site Manager may authorise employees to view digital media, but viewing is to be restricted to areas where it is appropriate to see the footage.

Employee requesting data relating to an employee incident.

21.11. Digital media (and associated data) relating to an employee incident may be saved by the Site Manager but is only to be shared with Director of HR or a Member of SLT.

For employee related incidents, online digital media may only be viewed by an employee with the authority of Director of HR, Director of Safeguarding, Campus Safeguarding Lead or a Member of SLT. Request from law enforcement

21.12. Law enforcement agencies, such as the Police, may request Digital media (and associated data) to assist in a specific criminal enquiry.

21.13. Digital media (and associated data) may be released to the Police, by the Exams and Compliance Manager, on receipt of an approved SAR form.

21.14. In the absence of an approved SAR, the Data Controller may give verbal consent for the Police to access digital media if it is judged that a delay in sharing may present a significant risk of harm.

21.15. Any person acting on behalf of the emergency services (Police) must present an official warrant card as proof of their identity before the disclosure of any data.

Request from an official representative

21.16. Digital media (and associated data) may be released to a solicitor and/or insurance company representative, by the Exams and Compliance Manager, on receipt of an approved SAR form.

Request from the individual affected

21.17. Digital media (and associated data) may be released to an individual affected (data subject), by the Exams and Compliance Manager, on receipt of an approved SAR form.

Media

21.18. Digital media (and associated data) shall only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Such a release shall be managed by the Exams and Compliance Manager.

21.19. Digital media (and associated data) shall not be released to the media for purposes of entertainment.

21.20. Materials or knowledge secured because of CCTV systems shall not be used for any commercial purpose.

Other parties

21.21. Unlike data subjects, third parties who wish to have a copy of digital media (images not of the person making the request) do not have a right of access to images under UK GDPR.

21.22. Digital media (and associated data) requested by other parties and for purposes outside the scope of this policy will not be permitted.

22. Breaches of this policy

22.1. Any suspected breach of this policy by college staff shall be considered under the college's disciplinary policy and procedures.

23. Data retention

23.1. Digital media (images & video) shall be retained for no longer than 31 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

24. Data disposal

24.1. Digital media (images & video) on electronic storage shall be erased by automated system overwriting.

24.2. All downloads, still photographs and hard copy prints shall be securely disposed of as sensitive waste. The date and method of destruction shall be recorded on the bottom of the original approval to copy held by the Site Manager.

25. Complaints

25.1. Complaints regarding the CCTV system and its operation shall be made under the college complaints procedure.

26. Training

26.1. The following training needs have been identified to ensure that all individuals affected by this document can effectively perform their duties:

26.1.1. All those involved in the management and operation of the CCTV system should be provided with suitable information, instruction, training and supervision relating to UK GDPR. Particular attention should be paid towards the management of Subject Access Requests (SAR).

26.1.2. Operators and maintainers should be provided with adequate training on the CCTV system, by a competent person, to enable them to carry out their duties effectively, with records kept. This training should be reviewed at regular intervals to ensure that it remains current.

26.1.3. All new employees should be made aware of this policy during the Human Resources (HR) core induction process.

26.1.4. All new members of a team should read this policy and confirm their understanding of their responsibilities within it.

26.1.5. Students should be made aware of the CCTV system and how it is designed to provide a safer environment for everyone within the college.

26.1.6. Adequate time within the term should be allocated to training to allow the CCTV system to be explained to all students.

27. Record keeping

27.1. The following records shall be created, developed, and maintained to demonstrate compliance with this document:

27.1.1. Risk assessment(s).

27.1.2. Subject Access Requests (SAR).

28. Governance & legislation

28.1. The following governance and legislation apply to this document and shall be routinely monitored for any changes:

28.1.1. The Data Protection Act 1998.

28.1.2. The UK General Data Protection Regulation (UK GDPR).

28.1.3. Freedom of Information Act 2000.

28.1.4. Protection of Freedoms Act 2012.

29. Associated documents

29.1. To gain a comprehensive understanding of this policy, it is essential to read the following documents in conjunction with it:

29.1.1. Security and Emergency Planning Policy.

29.1.2. Data Breach Notification Policy.

29.1.3. Data Protection Policy.

29.1.4. Disciplinary Policy.

29.1.5. Staff Code of Conduct Policy.

29.1.6. Comments, Compliments and Complaints Procedure.

29.1.7. Information Systems Acceptable Use Policy (Staff).

29.1.8. Estates CCTV Standard Operating Procedure.

29.1.9. Government information for setting up and using CCTV cameras.

29.1.10. Home Office Surveillance Camera Code of Practice.

30. Associated forms

30.1. The following forms are associated with this document:

30.1.1. Subject Access Request (SAR) Form.

31. Equality impact assessment

31.1. Wiltshire College & University Centre strives to ensure equality of opportunity for all staff, students and local people. As an employer and a provider of education, the college aims to ensure that none are placed at a disadvantage as a result of its policies and procedures. It is intended that this policy is fair to all. Where any part could potentially lead to unequal outcomes, the policy then justifies why this is a proportionate means of achieving a legitimate aim.

32. Data retention statement

32.1. Wiltshire College & University Centre is committed to ensure the data it collects, and holds is in line with the Information Commissioner's Office (ICO) guidance and meets data protection law. Where appropriate a Data Protection Impact Assessment will be undertaken as and when policies are updated to ensure risks to the individual and college are considered and managed.

32.2. For further information please refer to the Data Protection Policy.

33. Document management

33.1. The document administration table on the front cover of this document shall outline the essential information, such as:

33.1.1. Version control.

33.1.2. Document ownership.

33.1.3. Document review.

33.2. An electronic version of this document shall be saved on the college intranet (SharePoint) in Microsoft Word format. This shall be managed as the original (primary) copy and must not be amended without the permission of the document owner.

33.3. Copies of this document should only be shared in Adobe Pdf format to retain control of the content and layout.

33.4. Any printed version of this policy is provided for reference only and should be marked and managed as an uncontrolled copy. For the most up-to-date and accurate version, the reader should refer to the original (primary) copy saved on SharePoint.

34. Publication

34.1. This policy may contain sensitive security information so all versions, including hard copies and electronic versions (soft copies), should not be published in a public area without first seeking the permission of the document owner.

35. Audit and review

35.1. A formal review of this document shall take place at regular intervals, not exceeding a period of **36** months, by a competent person. It shall also be reviewed when:

35.1.1. There is a significant change to:

35.1.1.1. The Senior Leadership Team (SLT).

35.1.1.2. The organisation or role of the college.

35.1.1.3. The design or layout of the college.

35.1.1.4. Governance or legislation.

35.1.2. A significant incident has occurred.

35.2. The review process shall involve a thorough examination of the policy's content, its effectiveness, and its implementation, with any necessary updates or changes made to ensure it remains relevant and effective in promoting a safe and healthy workplace.

35.3. When updates are agreed and implemented, all changes shall be recorded in the amendment log table.

36. Document consultation

36.1. Consultations were conducted with the following key stakeholders during the development of this document:

36.1.1. Exams and Compliance Manager.

36.1.2. Finance and Maintenance Manager.

36.1.3. Head of Estates & Services.

36.1.4. Senior Site Manager.

36.1.5. H&S Manager.

35. Document feedback

35.1.1 Any comments on the accuracy or quality of this document, or suggestions for improvement, should be sent to the email address below, for the attention of: Finance and Maintenance Manager.

Email: estatesandservices@wiltshire.ac.uk