KMS 940 - Use of CCTV Policy

This document should be read in conjunction with

Information Commissions Office – In the picture: a data protection code of practice for surveillance cameras and personal information

Created By:	Deputy Principal (Finance & Corporate Services)	Next Review Date:	November 2024
Approved By:	SMT	Responsibility for Review:	Data Protection Officer / IT Team / H&S Manager
Date First Approved:	13 November 2014		

1. Purpose

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Kingston Maurward College, here after referred to as 'the College'.

The system comprises a number of fixed and Pan / Tilt / Zoom (PTZ) cameras located around the main College campus. All cameras are monitored from controlled Monitoring stations and are only accessible by selected staff on the Administrative Network.

This Policy follows Data Protection Act guidelines and the CCTV Code of Practice document issued by the Information Commissioner's Office (ICO), (see page 10 of the Code of Practice).

The CCTV system is owned by the College.

2. Objectives of the CCTV system

- To protect the College buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the College security

3. Forms Relating to this Policy

Form Description	**Document Ref**
Completed a College Evidence Release form	CEAR (KMS 860 refers)
Data Subject Access Request Form	DSAR
Monitoring Staff Declaration Form	MSD
CCTV Log of Viewings / Recordings	CCTV Log

These forms can be obtained from the KM Systems on Moodle or upon request from the Data Protection Officer (by email DPO@kmc.ac.uk or DataProtection@kmc.ac.uk)

4. Statement of Intent

The College's CCTV System will be registered with the Information Commissioner under the terms of the GDPR Act and will seek to comply with the requirements both of the Act and the Commissioner's Code of Practice.

The College will treat the system and all information, documents and recordings obtained and used, as data which is protected by the Act.

Cameras will be used to monitor activities within the College and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the College, Staff, Students and Visitors.

No static cameras are focussed on private homes, gardens and other areas of private property.

CCTV cameras are not, and will not, be used for the monitoring of teaching and learning.

Unless an immediate response to events is required, staff managing the system must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the College's forms for Directed Surveillance to take place, as set out in the Investigatory Powers Act (IPA) 2016 (replacement for the Regulation of Investigatory Power Act 2000).

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded images will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recorded images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect all incidents taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the College CCTV system.

5. Operation of the System

The System will be administered and managed by the Premises & Estates Manager in accordance with the principles and objectives of this Policy.

Responsibility for the day-to-day monitoring of the system and the responsibility for the management and maintenance of the system lies with the Premises & Estates Manager. The designated person can authorise others with the permission of the Principal to act as a deputy.

The CCTV system will be operated 24 hours each day, every day of the year.

Images are retained for a maximum of 30 days, once the 30th day has been reached the recordings are overwritten; however, most CCTV cameras are set to only retain images for 14 days*.

[*ICO website says organisations should have a retention policy. They should only keep the images for as long as necessary to meet the purpose of recording them.]

6. System Control

The Premises & Estates Manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

Unless an immediate response to events is required, staff utilising CCTV equipment must not direct cameras at an individual or a specific group of individuals.

Whilst footage is accessible from anywhere on campus, only authorised users have access to the monitoring system. Users are required to use system log-in credentials in order to access the system.

Hardware for the system is housed on campus, in a secure and locked area, access to which is managed by the IT Department.

7. Monitoring Rooms (Image Viewing Rooms)

Monitoring rooms are designated as room where live CCTV images can be monitored and management of the system can be performed. This includes the downloading of images to be transmitted via encrypted email.

The following is a list of the primary Monitoring Rooms:

- Estates Office (All areas)
- Security Office
- IT Office

All monitoring staff in each of these areas, but not exclusively restricted to these areas, must comply with the following procedures:

- All monitoring staff must read and understand the College's CCTV Policy and ICO Code of Practice and subsequent updates

- All monitoring staff must sign the "Monitoring Staff Declaration Form" to indicate they have read the Policy and agree to abide by the policies and procedures set out for the CCTV systems use.
  Form Reference: MSD.

All monitoring staff will adhere to the GDPR Protection Act and the Investigatory Powers Act (IPA) 2016. Copies of these acts can be found on the ICO website at http://www.ico.gov.uk

All monitoring staff must ensure that all CCTV images are kept private and not on general view within their Monitoring Rooms.

8. Monitoring & Digital Recording Evidence Procedures

Where images are required for evidential purposes in legal or College disciplinary proceedings, a link is created and saved in a protected file. All evidence must be gained within 7 days of the event. The link will only be sent to those that require it, and in an encrypted format.

Recorded images may be viewed by the Police for the prevention and detection of crime.

The authorised Police Officer must have completed the following:

- Completed a College Evidence Release form.
  Form Reference: CEAR (KMS 860 Refers)

- Produce an authorisation letter from his/her superior.
  This should be copied and retained with the College Evidence Release form – CEAR (KMS 860 Refers)

A CCTV log will be maintained of the viewing of Recorded images by the police and the release of Recorded images to the Police or other authorised applicants.

Requests by the Police can only be actioned under section 29 of the GDPR Act. Recorded images will only be released to the Police on the clear understanding that the image copy remains the property of the College.

The College also retains the right to refuse permission for the Police to pass to any other person the image copy or any part of the information contained thereon. On occasions when a Court requires the release of an image copy, this will be produced from the secure evidence previously taken.

The Police may require the College to retain the stored recorded images for possible use as evidence in the future. Such recorded images will be properly indexed and securely stored until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release recorded images will be referred to The Principal. Recorded images will only be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

9. Breaches of the Policy (including breaches of security)

Any breach of the Policy, including the ICO Code of Practice, by College staff will be investigated by a member of the Senior Management Team.

Any serious breach of the Policy, including the ICO Code of Practice, will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Complaints

Any complaints about the College's CCTV system should be addressed to the College Complaints Officer who will then liaise with the Data Protection Office.

Complaints will be investigated and issues arising from the investigation will be addressed accordingly and the relevant remedial action taken.

11. Access by the Data Subject

The GDPR Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including that obtained by CCTV.

Requests for Data Subject Access should be made on the application form available from the IT Services or Estates department. Form Reference: DSAR.

12. Public information

Copies of this Policy including the ICO Code of Practice will be available to the public from the College website.

Evidence access release form CEAR

GDPR Act

Request for disclosure of personal data under the GDPR Act (Formerly s29 Data Protection Act)

This form will be used to help the College identify the footage you have requested.
Please complete the form and send it to the address at the end of the form. All fields marked * are mandatory.

1 Details of applicant	
*Name	
*Rank and collar number	
*Organisation	
*Address or e-mail address	
Telephone number	
2 Details of request	
Please provide an encrypted copy in respect of the following:	
*Location(s)	
*Building Name / Camera Name	
*Date(s)	
*Time(s)	
*Description of incident/person(s)	
*Reason why this information is needed for the purposes of preventing or detecting crime/brief details of enquiry	

3 How would you like to receive the information?	
We normally provide copies of CCTV footage via encrypted email. Please could you state how you would like to receive the requested information?	
Preferred email address	
Come in to collect DVD	
Sent by post (recorded delivery) to address in section 1	

4 Declaration	
I understand that if any of the information given on this form is knowingly incorrect, I may be committing an offence under the terms of the GDPR Act 2018	
***Signed:** ***Name:**	***Rank and collar number:** ***Date:**
***Authorising signature:** (at least rank of Inspector) ***Name:**	***Rank and collar number:** ***Date:**

5 For office use only	
I hereby authorise ☐ refuse ☐ the disclosure of the images in relation to the above location(s), date(s) and time(s).	
Signed:	
Date:	

Reasons for refusal (if applicable)

Request for access to information DSAR

Data Protection Act

CCTV Subject Access Request Form

This form is used to confirm the identity of the data subject, the identity of any representatives if applicable, and for you to tell us what footage you require. Please complete this form below providing as much detail as possible to help the council to identify and locate the information requested. An asterisk (*) indicates a required field, as without these the council will be unable to process your request. Please complete it and send it to the address at the end of the form.

1 Details of data subject (person in the footage)	
Title	
*First name	
*Surname	
*Address / or email address	
Telephone number	

General Data Protection Act

Kingston Maurward College will treat your personal information in line with the GDPR Act. In particular, the information you provide on this form will be used to monitor and fulfil your request. It will not be shared with any third parties, kept securely and will not be used for any other purpose.

2 Details of request
*Please use this section to tell us any other details that may help us to locate the footage required, for example date, time, location, and a description of the data subject. The more specific you can be the easier it will be for us to find the information. Please note that we only retain footage for 14 days after it has been recorded.

3 Details of applicant

PART 1

Are you the data subject (the person in the footage)?

Yes? ☐ If you are the data subject we will need to verify your identity. Please supply photographic evidence to support this (e.g. photocopy of passport, driving licence etc). **[PLEASE SIGN THE DECLARATION ON THE NEXT PAGE]**

No? ☐ If you are not the data subject we will need to ensure that are you acting on behalf of the data subject with their written authority. Written authority must be enclosed with this request form together with evidence of your identity and that of the data subject. **[PLEASE NOW COMPLETE PART 2]**

For official use only – I confirm identity

Name	
Job title	
Date	

PART 2

If you are not the data subject, then please complete this section, otherwise proceed to the declaration.

*Name	
Organisation (if applicable)	
*Address	
E-mail address	
*Relationship to the data subject	
Telephone number	
*Written authority enclosed	

4 Receiving the Information	
We normally provide copies of CCTV footage via encrypted email. Please could you state the email contact details required	
Contact Email Address:	

5 Declaration

To be completed by all applicants. Please note that any attempts to mislead may result an offence under section 55 of the Data Protection Act and may lead to prosecution

*I (insert name) _____

certify that the information given on this subject access request form to Kingston Maurward College is true to the best of my knowledge. I understand that it is necessary for Kingston Maurward College to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct data. I understand that the information given on this form may be passed to the relevant departments in order to locate the data, but it will not be used for any unrelated purpose nor shared with any other organisation.

Please note that in the event that information supplied would seriously prejudice the prevention or detection of crime, Kingston Maurward College have the right under the Data Protection Act to refuse requests for access.

Kingston Maurward College has 40 calendar days from the date of receipt of the request to respond to this request.

The footage requested may relate to a third party, where this is the case, that data may have the third party information removed.

*Signature:	*Date:

Please return this form to:
Data Protection Officer
Kingston Maurward College
Dorchester
Dorset
DT2 8PY

Or if you wish to bring proof of identity in to the College, please contact:
01305 215000
dataprotection@kmc.ac.uk

Please remember to enclose proof of your identity.

Documents which must accompany this application:

1) Proof of identity
2) Written authority if requesting in behalf of the data subject
3) Photographic evidence to support confirmation of identity

We strongly recommend that you send your form and documents by a secure method, for example recorded delivery.

For Office use only

Date Request Received:	
Name:	
Job title:	

CCTV – Monitoring Staff Declaration Form MSD

CCTV Monitoring Staff Declaration Form

All employees that are authorised to view the CCTV images within Kingston Maurward College must read this protocol alongside the Policy for use of CCTV and confirm that they understand and agree to abide by the policy and protocol.

- CCTV images may only be viewed/copies made by authorised employees as necessary.
- All authorised employees viewing the CCTV images will act with utmost probity at all times and all images viewed must be treated as confidential and should not be used for any personal use.
- All authorised employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.
- Access to view any particular images to Member of staff with direct involvement in an incident must be noted on the CCTV log sheet.
- Any copies of images made for investigation purposes should be logged on the CCTV log sheet and should not be retained for longer than is necessary and destroyed securely.
- All authorised employees are responsible to ensure that CCTV images are not left on any screen without an authorised employee being left in charge. An authorised employee should log out of the programme when leaving the screen.
- Every viewing of the images will accord with the purposes and key objectives of the CCTV system and shall comply with the CCTV Policy.
- All authorised employees viewing CCTV images should be aware of exercising prejudices, which may lead to complaints of the system being used for purposes other than those for which it is intended. The viewers may be required to justify their interest in any particular individual, group of individuals or property at any time.
- Any breach of the Policy for the use of CCTV will be dealt with in accordance with existing discipline regulations. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.
- Any breach of the Data Protection Act will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this act.

I understand and agree to abide by the Policy for the Use of CCTV and the CCTV Protocol

NAME _____ **JOB TITLE** _____

SIGNATURE _____ **DATE** _____

KINGSTON MAURWARD COLLEGE - CCTV LOG OF VIEWINGS / RECORDINGS							
Event No	Event Date & Time	Recording Date & Time	Reason	Copy Taken By / Viewed By	Signature	Authorised By (if applicable)	Signature Confirming Destruction (if applicable)

- **This page has been left blank intentionally**