KINGSBRIDGE COMMUNITY COLLEGE

CCTV Policy

Approved by KCC Governors:	**25th June 2024**
Version:	**0.3**
Author Initials:	**TGR**
Review Date:	**June 2027**

Contents

1. Principles and Introduction

1.1. As a college we have a responsibility to provide a safe environment within which children can learn. We believe that every effort should be made to safeguard children's wellbeing and ensure that steps are taken to discourage individuals from posing a risk to KCC students or the environment within which they learn. Kingsbridge Community College has installed and maintains a CCTV system in order to protect against vandalism, crime, antisocial behaviour and to protect students, staff, parents and members of the public when they are on College premises.

1.2. This policy is to enable the College to comply with the Data Protection Act (1998), the Human Rights Act (1998), the Protection of Freedoms Act (2012) and the subsequent code of practice released by the Information Commissioner's Office (2015),

1.3. This policy applies where open use of CCTV is intended in public areas. It does not apply to targeted or covert surveillance activities.

1.4. This policy will be reviewed as appropriate or as legal advice changes.

2. Responsibilities for CCTV operation

2.1. The CCTV scheme is administered and managed by the Principal, the Site Supervisor and the IT Services Manager in accordance with this policy and with guidance from the Department for Education (DfE) where necessary.

2.2. The day-to-day management of the CCTV scheme is the responsibility of the Principal, Senior Leadership Team, Raising Standards Leads and Inclusion Leads.

2.3. Precautions are in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to any guidance or security precautions.

3. Legal basis for use of CCTV systems

3.1. The use of CCTV and the images recorded will comply with the Data Protection principles and will be:

- Fairly and lawfully obtained;
- Adequate, relevant and not excessive;
- Accurate;
- Used only for purposes about which people have been informed;
- Secure and protected from unauthorised access;
- Not held longer than required for the purposes for which they were recorded;
- Accessible to data subjects where a request has been made under the Data Protection Act and where the images are defined as personal data.

3.2. The purposes for which CCTV is in use across the College are the following:

- Prevention and detection of crime, eg. theft, arson, criminal damage and vandalism;
- To protect the College buildings and assets;
- To increase the perception of safety and reduce the fear of crime;
- To assist in the management of the College when constant supervision is not possible;
- To protect members of the public and private property;
- To ensure the safety of students and others present on KCC premises and enhance positive behaviour of students, staff and visitors.

3.3. The use of CCTV will be fair and not be excessive or prejudicial to any individual or any group of individuals. The College will inform people that CCTV is in use on the premises by means of notices.

4. Ensuring that use of CCTV is fair

4.1. The College will include the use of CCTV on its annual Data Protection notification (registration) to the Information Commissioner's Office as one of the purposes for which it uses personal data.

4.2. The College will only use CCTV for the purposes stated. CCTV or images produced from it will not be used for any other purposes, particularly purposes which could not reasonably be envisaged by individuals.

4.3. The College will ensure that students, staff and other people who use its buildings are informed of the use and purpose of CCTV. This will be done by means of clear and obvious notices placed around College premises. Notices will include the following information:

- The identity of the Data Controller;
- The purposes for which CCTV is being used, eg. for the prevention or detection of crime or to increase safety and security whilst on College premises;
- Details of who to contact about the scheme and name/phone number where applicable.

4.4. CCTV cameras will only record images on College premises and will not be directed at surrounding private property.

5. Security

5.1. CCTV viewing access will be strictly confined to authorised staff. Where other staff or visitors need to have access to the system, this will be documented.

5.2. If out of hours' emergency maintenance of CCTV equipment is required, the staff member in charge of the CCTV system must be satisfied of the identity of contractors before allowing access to the equipment.

5.3. Retention of recordings: recordings made will be held for a limited length of time and will be destroyed when their use is no longer required. The maximum period is normally 28 days but this may be extended where the recordings are required for an ongoing investigation or where an ongoing issue means an historic record is deemed necessary. When the retention period has been reached, digital recordings or removable media will be destroyed or wiped securely.

6. Location

6.1. Cameras are located in those areas where the College has identified a need and where other solutions are ineffective. The College's CCTV system is used solely for purposes identified above and is not used to routinely monitor student or staff conduct.

7. Covert Surveillance

7.1. The College does not use the CCTV system for covert monitoring. Should the College need to use CCTV covertly (ie, without making people aware of it), an application will be made under the Regulation of Investigatory Powers Act (RIPA).

7.2. The College will discuss the matter with its solicitors to ensure appropriate guidelines are followed.

7.3. Where the police wish to undertake covert surveillance, they will gain authorisation from their own Single Point of Contact (SPOC).

8. Procedures for disclosure of CCTV records to other organisations

8.1. Access to CCTV recordings day-to-day will be restricted to staff who operate the system.

8.2. CCTV recordings will be held only by the College unless there is a legitimate reason to disclose them. Disclosure includes the viewing of images by someone who is not the operator of the system as well as the transfer of recordings to another organisation.

8.3. Records may need to be disclosed for the following reasons:

- To the police, for the prevention and detection of crime;
- To a court for legal proceedings;
- To a solicitor for legal proceedings;
- To the media for the purposes of identification.

8.4. Where recordings have been disclosed or viewed by an authorised third party the College will keep a record of:

- When the images were disclosed;
- Why they have been disclosed;
- Any crime incident number to which they refer;
- Who the images have been viewed by or disclosed to.

8.5. Viewing of CCTV recordings by the Police will be recorded in writing. Requests by the Police are actioned under Section 29 of the Data Protection Act. The Police should provide a completed Section 29 form stating that the information is required for the prevention and detection of crime. If a form is not available, or in an emergency, the College must record in writing when and why the information has been released.

8.6. Should a recording be required as evidence, a copy may be released to the Police. Where this occurs the recording will remain the property of the College. The date of the release and the purpose for which it is to be used will be recorded.

8.7. The Police may require the College to retain recordings for possible use as evidence in the future. Such records will be stored and indexed so that they can be retrieved when required.

8.8. Applications received from other outside bodies (eg, solicitors) to view or release recordings will be referred to the Principal. In these circumstances, recordings may be released where satisfactory evidence is produced showing that they are required for legal proceedings, an information access request (see section 7) or in response to a Court Order.

8.9. Recordings will only be released to the media for use in the investigation of a specific crime and with the written agreement of the Police.

9. Subject Access Requests

9.1. Under Section 7 of the Data Protection Act 1998, individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Act. If a request is received, a fee (up to a maximum £10) can be charged and a copy of the images must be provided within 40 days of the request.

9.2. Recent legal cases have raised the issue of when CCTV images should be considered as personal data. Guidance arising from this implies that personal data must be substantially about the person and should affect their privacy in some way. In relation to CCTV this will not include all images:

- A wide shot of an outdoor space or College corridor with many people in view of the cameras would not normally be considered as the personal data of all those involved. However, where a camera has picked up an individual or group of individuals specifically, or has been moved to focus in on them, the images recorded can be considered personal data.

9.3. Where a request has been made to view an image or recording, an application must be made in writing. The individual may wish to access either a still image or part of a recording. Where third parties are included in the shots, they will be removed where this is technically possible. Where removal is not possible, their consent will be sought. Where consent is refused or where it is not possible to gain consent, a balanced decision will be made, taking conflicting interests into account, as to whether it is reasonable in all circumstances to release the information to the individual.

9.4. There is no obligation to provide information where a request has been made after CCTV records have been routinely destroyed in accordance with this policy - see section 3 (ie, for recordings that no longer exist). However, where a request has been made for recordings still in existence, they will not be destroyed until the request is complete.

10. Breaches of Policy

10.1. Any breach or alleged breach of this policy or College guidelines on the use of CCTV by College staff or other individuals will be investigated by the Principal.

10.2. An investigation will be carried out into any breaches of policy and procedures reviewed or put in place to ensure that the situation does not arise again.

11. Complaints

11.1. Any complaints about the operation of the CCTV system should be addressed to the Principal, where they will be dealt with according to the College's standard complaints procedures, with reference to this policy and the College's Data Protection policy.

12. Review of the CCTV Policy

12.1. The policy is reviewed every 3 years (and/or following a change in legislation or ICO guidance) by the Governing Body.