King's Worcester

CCTV Policy

1. Introduction

The King's School, Worcester (the Foundation) uses CCTV cameras to view and record pupils, parents/guardians, staff and visitors on and around our premises in order to maintain a safe environment for all, and to protect school property. This policy relates to the use and management of CCTV throughout the Foundation premises and should be read alongside our Data Protection Policy and Data Retention Policy.

We recognise that the images of individuals recorded by CCTV cameras are personal data which must be processed in accordance with applicable data protection legislation (as defined below) as well as the Information Commissioner's Office (ICO) CCTV guidance relating to the use of video surveillance. As a Data Controller, we have notified our use of personal data (which includes CCTV) with the ICO and seek to comply with its best practice guidance.

The purpose of this policy is to:

- outline why and how we will use CCTV, and how we will process personal data recorded by CCTV cameras
- ensure that the legal rights of our pupils, parents/guardians, staff and visitors relating to their personal data are recognised and respected
- assist staff in complying with relevant legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence; and
- explain how to make a Subject Access Request (SAR) in respect of personal data created by CCTV.

The CCTV System (the system) is administered and managed by the Foundation, which is the Data Controller in respect of personal data collected by our CCTV cameras. If you have any questions about this policy, please contact the Director of Operations.

The Foundation will review the ongoing use of existing CCTV cameras regularly to ensure that their use remains necessary and appropriate, and that the system is continuing to address the needs that justified its introduction.

We take compliance with this policy very seriously. Failure to comply puts at risk the individuals whose information is being processed, carries the risk of significant civil and criminal sanctions for the individual and for the Foundation, and may, in some circumstances, amount to a criminal offence by the individual. As a result, breach of this policy may be treated as a disciplinary matter and, following investigation, may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

All fixed cameras are in plain sight on the Foundation premises and the Foundation does not routinely use CCTV for covert monitoring or monitoring of private property outside the Foundation grounds. Where cameras cover third party property within their view that third party property is obscured as far as is reasonably practicable within the CCTV software.

2. Accessibility

The King's School, Worcester is committed to making our policies accessible to everyone. If you require this document in an alternative format - such as large print, Braille, audio, or another language - please contact the Foundation via info@ksw.org.uk or by telephone on 01905 721700. We will do our best to provide the information you need in a way that works for you.

3. Definitions

For the purposes of this policy, the following terms have the following meanings.

Biometric Data: means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, as defined at Article 4(14) UK GDPR.

CCTV: means fixed and domed cameras designed to capture and record images of individuals and property both indoors and outdoors.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data subjects: means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Personal data: means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

Data Controllers: are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. The Foundation is the Data Controller of all personal data used in our schools for our own purposes.

Data users: are members of staff whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

Data processors: are any person or organisation that is not a data user (or other employee of a Data Controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

Data Protection Legislation: means the Retained Regulation (EU) 2016/679, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), and related laws including but not limited to, the Human Rights Act 1998.

Processing: is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

Surveillance systems: means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future that captures information of identifiable individuals or information relating to identifiable individuals.

4. Objectives

The Foundation's purposes for using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the Foundation believes these purposes are all in its legitimate interests; as well as being reasonable, appropriate and proportionate. For ease of reference, CCTV systems are deployed at our premises on the legal basis set out in our Privacy Notices. Data captured for the purposes below will not be used for any commercial purpose.

- To protect pupils, staff and visitors with regard to their personal safety and to act as a deterrent against crime.
- To protect the Foundation buildings and equipment, and the personal property of pupils, parents/guardians, staff and visitors from damage, disruption, vandalism and other crime.
- To prevent and detect crime, and support law enforcement bodies in the prevention, detection and prosecution of crime and as well as the identification and apprehension of offenders.
- To monitor the security and integrity of the Foundation sites and deliveries and arrivals, including car and number plate recognition.
- To protect staff and contractors when carrying out work duties.
- To monitor and uphold discipline among pupils in line with the School Rules, which are available to parents/guardians and pupils on request.
- To assist in day-to-day management, including ensuring the health and safety of pupils, parents/guardians, staff and visitors.
- To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.
- To assist in civil litigation, including employment tribunal proceedings.

Please note that this list is not exhaustive, and other purposes may become relevant as set out in our Privacy Notices.

The CCTV system will not be used to:

- record sound unless in accordance with the policy on covert recording (see below)
- for any automated decision taking
- monitoring private and/or residential areas or premises.

Before installing and using CCTV systems on our premises, we have:

- assessed and documented the appropriateness of and reasons for using CCTV
- established and documented who is responsible for day-to-day compliance with this policy

- ensured signage is displayed to inform individuals that CCTV is in operation, and that CCTV operations are covered in appropriate policies.

We keep a record of the CCTV installed and used.

Once installed, reviews will be regularly undertaken to ensure that the use of CCTV systems and the processing of personal data obtained through it remains justified.

5. Monitoring

The CCTV System will be operational 24 hours a day, every day of the year.

The System Manager (defined below) will check and confirm that the system is properly recording and that cameras are functioning correctly, on a regular basis.

The CCTV system will be checked and (to the extent necessary) serviced no less than annually.

Locations have been selected, both inside and out (including corridors and common rooms as appropriate), that the Foundation reasonably believes require monitoring to address the stated objectives.

These locations have been chosen to minimise viewing of spaces not relevant to the legitimate purposes of the Foundation's monitoring. As far as practically possible, CCTV cameras will not focus on private property; and no images of public spaces will be captured except to a limited extent at site entrances and adjacent walkways, pavements and roadsides. In addition, surveillance systems will not be used to record sound and no images will be captured from areas in which individuals would have a heightened expectation of privacy, including medical, changing and washroom facilities.

How we will operate any CCTV

Adequate signage has been placed in prominent positions, at all entrance points to the Foundation and in the vicinity of the cameras, to inform staff, pupils, parents/guardians and visitors that they are entering a monitored area. The CCTV signs will state:

- that we are responsible for CCTV recording (identifying the Foundation as the Data Controller)
- the legal purpose(s) of the CCTV recording and how recording may be used
- how long recordings will be kept
- that individuals can access recordings
- contact details for further information regarding the CCTV system.

We will ensure that recorded images are only viewed by approved members of staff whose roles require them to have access to such data. This may include the Estates Manager, Caretaker(s), Senior Leadership Team and relevant staff on duty. Staff using the system will be given appropriate training to ensure that they understand and observe the legal requirements related to the processing of relevant data.

Images will only be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of, or opportunity for, access to unauthorised persons.

Data and image Retention

The day-to-day management of images will be the responsibility of the Estates Manager who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered by CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data where it is possible to do so. Given the large amount of data generated by the CCTV system, we may store video footage using a cloud computing system. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards. We may also engage data processors to process data on our behalf. We will ensure appropriate contractual safeguards are in place to protect the security and integrity of the data.

Images and recording logs will be retained and disposed of in accordance with our Data Protection Policy and Data Retention Policy. Images stored on removable media will similarly be erased or destroyed once the purpose of the recording is no longer relevant.

Where personal data is retained, it will be held in accordance with the Data Protection Act 2018 and our Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log.

6. Retention and erasure of data gathered by CCTV

Images will be stored for the duration available on the system hard drive (normally 2-4 weeks) and automatically over-written unless the Foundation considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.

Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images have been authorised to be used for any disciplinary purpose or other legal reason, the footage must be retained securely in the relevant case file. The retention period for this file is set out in our Data Retention Policy.

At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes, discs, still photographs and/or hard copy prints will be disposed of as confidential waste. We will maintain a log of when data is deleted.

7. Use of additional surveillance systems

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate and may carry out a Data Privacy Impact Assessment (DPIA).

A DPIA is intended to assist the Foundation in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, the Foundation will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

The Foundation will confine CCTV to areas where expectations of privacy are low. No surveillance cameras will be placed in areas where there is an increased expectation of privacy (for example, in changing rooms or toilets) unless, in very exceptional circumstances, it is judged to be necessary to deal with very serious concerns. In this situation the Foundation will always complete a DPIA and have regard to it before deciding whether to proceed.

8. Covert monitoring

Covert monitoring means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place.

The Foundation will never engage in covert monitoring or surveillance unless, in very limited and highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or serious malpractice is taking place and, after suitable consideration (including the completion of a DPIA), it is reasonable to believe there is no less intrusive way to tackle the issue. If necessary, the Foundation will only undertake covert recording in accordance with the Data Protection Laws and ICO guidelines.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Head of Foundation following receipt of advice from the Director of Operations/Compliance Manager. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on individuals will always be a primary consideration in reaching any such decision. Our Director of Operations/Compliance Manager will have regard to the completed DPIA when making their decision.

Only limited numbers of people will be involved in any covert monitoring as necessary.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity. Its use should be immediately stopped when that specific investigation has been completed. Any decision to use covert surveillance for any reason must be fully documented and records of such decision retained securely.

9. Requests for Disclosure

Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

No images from our CCTV cameras will be disclosed to a third party without express permission being given by the Foundation. Data will not normally be released unless satisfactory evidence is given that it is lawful to do so. The following are examples of circumstances when the Foundation may authorise disclosure of CCTV images to third parties:

- where required to do so by the Head of Foundation, Prep School Heads, the Police or any relevant local or statutory authority
- to make a report regarding suspected criminal behaviour or a Safeguarding incident
- to enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern
- to assist the Foundation in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the Foundation's management of a particular incident
- to individual data subjects (or their legal representatives) pursuant to a subject access request (as outlined above)
- to the Foundation's insurance company where required in order to pursue a claim (for example for damage done to insured property); or
- in any other circumstances required under law or regulation, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

Where images are disclosed, a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed, the location to which any footage is being transferred to (if footage/images are being removed from the CCTV system), the signature/written confirmation of receipt of the person to whom the images have been transferred and a crime incident number (if applicable).

The Foundation reserves the right to obscure images of third parties when disclosing CCTV footage, where we consider it necessary to do so.

No images from CCTV will ever be made public (including posting online) or disclosed to the media.

10. Subject Access Requests (SAR)

Individuals also have the right to request access to personal data that the Foundation holds about them, known as a Subject Access Request (SAR) (please see the Foundation's Data Protection Policy for further information), including information collected by the system, if it has been retained. It will be handled in line with data protection law and our applicable policies and procedures.

In order to respond to a SAR, the Foundation will require specific details including (as a minimum) the time, date and camera location and if necessary, information identifying the individual (e.g. what they were wearing) in order to locate the relevant footage.

The Foundation may be required or permitted to obscure images of third parties (i.e. other individuals) when disclosing CCTV or other footage as part of a SAR. We may also offer for you to view the footage on school premises if appropriate. The Foundation must also be satisfied to the identity of the person wishing to view stored images and the legitimacy of the request.

If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

11. Requests to prevent processing

The Foundation recognise that, in certain circumstances, we may be required to stop processing personal data, if an individual requests it. Under data protection law individuals also have other legal rights with respect to their data as listed and set out in our Privacy Notice. For further information regarding this, please contact our Compliance Manager at compliance@ksw.org.uk.

12. Other CCTV systems

The Foundation does not own or manage third party CCTV systems but may be provided by third parties with images of incidents where this is in line with the objectives of the Foundation's own CCTV policy and/or its School Rules.

Many pupils travel to the Foundation on coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The Foundation may use these in establishing facts in cases of unacceptable pupil behaviour, in which case the parents/guardian will be informed as part of the Foundation's management of a particular incident.

13. Complaints and queries

If you have any queries or complaints in relation to the Foundation's use of CCTV, your personal data, requests for copies, or any question about this policy, please contact the Foundation's Director of Operations via:

Email: compliance@ksw.org.uk

Telephone: 01905 721721

Post: The King's School, 5 College Green, Worcester, WR1 2LL.

If you are not satisfied with the response received, you are entitled to contact the ICO. Details of how to do this can be found on the ICO website: www.ico.org.uk.

14. Enforcement and Compliance

All authorised users of the Foundation's surveillance technology and its underlying data are required to adhere to the controls around the use of CCTV as set out in this policy and as may be advised separately from time to time. The use of the CCTV systems for any other purpose other than those specifically authorised will be subject to a full investigation and could lead to disciplinary action up to and including dismissal without notice.

The misuse of our surveillance systems and unauthorised use of images and CCTV footage may constitute a criminal offence.

15. Approval

The Governing Body will review and approve significant policy changes annually or at more frequent intervals if there are relevant legislative changes, and/or the evaluation of the policy highlights the need for a review.

Version No	Approval Date	Approval Confirmed by
1	28 March 2025	Pat Preston, Chair of Governors
2	27 March 2026	Pat Preston, Chair of Governors

16. Version Control

Version No	Date	Summary of changes	Reviewed by
1	27/02/2025	Policy checked to the latest ISBA standards published October 2024.	Adam Winter, Director of Operations
2	09/02/2026	No updates to policy. Addition of Version Control tracking.	Adam Winter, Director of Operations