MALVERN ST JAMES
Girls' School

Closed Circuit Television (CCTV) Policy

This policy is the responsibility of the Director of Operations and Compliance to review and update annually.

Purpose and Scope

At Malvern St James we use CCTV cameras to view and record individuals on and around the School site in order to maintain a safe environment for pupils, staff and visitors, and to protect school property. This policy relates to the use and management of CCTV throughout the school premises and should be read alongside our Data Protection 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's (ICO's) 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 data recorded by CCTV cameras;
- ensure that the legal rights of staff pupils, parents, volunteers, visitors to the school and members of the public, relating to their personal data, are recognised and respected;
- assist staff in complying with their own 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 in respect of personal data created by CCTV.

This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

We take compliance with this policy very seriously. Failure to comply puts at risk the individual whose information is being processed, carries the risk of significant civil and criminal sanctions for the individual and for us, 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.

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 , physio-logical 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;

- **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. We are the data controller of all personal data used in our School for our own purposes;
- **Data users**: are those of our employees 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 capture information of identifiable individuals or information relating to identifiable individuals.

Reasons for the use of CCTV

We have considered and determined that the purposes for which CCTV is deployed are legitimate, reasonable, appropriate and proportionate. For ease of reference, CCTV systems are deployed at our premises on the legal basis set out in our Privacy Notice and its purpose is in order to:

- deter crime and assist in the prevention and detection of crime and/or serious breaches of policies and procedures;
- protect buildings and assets from damage, disruption, vandalism and other crime;
- assist with the identification, apprehension and prosecution of offenders;
- for the personal safety of pupils, staff, volunteers, visitors and other members of the public;
- to assist in day-to-day management, including ensuring the health and safety of staff and others;
- to monitor the security and integrity of the School site, associated deliveries and arrivals, and car parking;
- to monitor staff and contractors when carrying out work duties; and
- to monitor and uphold discipline among pupils in line with the School's Code of Conduct and other policies, which are available to parents and pupils on request.

This list is not exhaustive and other purposes may be or become relevant as set out in our Privacy Notice.

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; or
- 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; and
- 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.

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

Monitoring

CCTV monitors the main building external perimeter and the external entrance doors to the main building. It is operational 24 hours a day and this data is continuously recorded OR during working hours only and this data is recorded.

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property. Surveillance systems will not be used to record sound.

Images are monitored by authorised personnel. Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of video and images captured by CCTV on site.

How we will operate any CCTV

Where CCTV cameras are placed in the workplace, we will ensure that signs are clearly displayed in the vicinity of the cameras to alert individuals that their image may be recorded. Our CCTV signs will state:

- that we are responsible for CCTV recording;
- 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; and
- contact details for queries regarding the CCTV scheme.

Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include Night Security Wardens as part of their security duties, the ICT Manager as part of the management of the system and HR staff involved with disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

Data and Image Retention

Images and recording logs must be retained and disposed of in accordance with the Data Protection Policy. Images stored on removable media will similarly be erased or destroyed once the purpose of the recording is no longer relevant. Data will only be retained for legal and/or compliance reasons in accordance with the relevant Data Protection Policy.

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from 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 surveillance systems, 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 engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

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 the School's Data Protection 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.

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 by carrying out a data privacy impact assessment (**DPIA**).

A DPIA is intended to assist us 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, we 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 School 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 by us to be necessary to deal with very serious concerns.

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.
We 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 within the workplace and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue. If necessary, we 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 following receipt of advice from the Data Protection Officer. 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 innocent workers will always be a primary consideration in reaching any such decision.

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

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.

Requests for disclosure

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Data Protection Officer. Data will not normally be released unless satisfactory evidence is given that it is lawful to do so, e.g. when it is required for legal proceedings or under a court order.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage, including the location to which the footage are being transferred to (if footage/images are being removed from the CCTV system), any crime incident number (if applicable) and the signature / written confirmation of receipt of the person to whom the images have been transferred.

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

Subject access requests

Data subjects may make a request for disclosure of their personal information and this may include CCTV images subject access request. A subject access request should be made in writing in accordance with our Data Protection Policy (available within the Staff Handbook) and it will be handled in line with data protection law and the School's applicable policies and procedures.

In order for us to locate relevant footage, any requests for copies of recorded CCTV images should normally include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual (e.g. what they were wearing).

We 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 subject access 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.

Requests to prevent processing

We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making. For further information regarding this, please contact the Data Protection Officer.

Complaints

If any member of staff has any concerns about our use of CCTV, they should speak to the Data Protection Officer in the first instance. Where this is not appropriate, or matters cannot be resolved informally, employees should use the School's formal Grievance Procedure (available within the Staff Handbook).
If a complainant or enquirer is not satisfied with the response received, they are entitled to write to the ICO. Details of how to do this can be found on the ICO website: www.ico.org.uk.

Enforcement and Compliance

All authorised users of our 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.

Any concerns regarding the use of CCTV should be shared with the School's Data Protection Officer.

Authorised by Governors of Malvern St James

Signature

Date 28 November 2023

Effective date of the policy	28 November 2023
Review date	Autumn Term 2024
Circulation	Governors / Staff / parents / pupils [on request]

Appendix 1

CCTV FOOTAGE ACCESS REQUEST

The following information is required before the School can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the school typically deletes CCTV recordings after 3 weeks.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date and time of footage sought	
Approximate time (give a range if necessary)	

Signature*……

Print Name……. Date ……..

*** NB if requesting CCTV footage of a child (under 12/13), a person with parental responsibility must sign this form. For children over 13, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.**