



LOCKERS PARK SCHOOL

CCTV AND SURVEILLANCE SYSTEMS

POLICY

Date Last Updated	By...	Date of next review
September 2024	GT	September 2025
May 2025	NC	May 2026
August 2026	NC	August 2027

1. Purpose and Scope

We use CCTV cameras to view and record individuals on school minibuses, in centralised locations within the school buildings and within the Quiet Room 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 on school property and should be read alongside our Data Protection Policy, our Data Retention Schedule, our Child Protection and Safeguarding Policy, our Staff Privacy Notice and our Pupil and Parent Privacy Notice.

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 data recorded by CCTV cameras;
- ensure that the legal rights of pupils, parents, staff and visitors, 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. Whilst it places obligations on staff, it also applies to our processing of the personal data of pupils, parents and visitors, who have the same rights under it.

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 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.

2. 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 UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA 2018**), in each case as amended by the Data (Use and Access) Act 2025 (DUAA), and related laws including but not limited to the Human Rights Act 1998 and the Protection of Freedoms Act 2012.

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.

3. 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 and on school minibuses on the legal basis set out in our Privacy Notice and its purpose is in order to:

- protect the personal safety of pupils, staff and visitors;
- assist in day-to-day management, including ensuring the health and safety of staff and others;
- assist internal investigations.

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)
- carry out any automated decision-making within the meaning of Articles 22A to 22D UK GDPR;
- monitor private and/or residential areas or premises; or

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 (where relevant) 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. The School is not a “relevant authority” for the purposes of the Protection of Freedoms Act 2012, but as a matter of good practice we have regard to the twelve guiding principles of the Surveillance Camera Code of Practice issued under that Act, which remains in force.

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.

4. Monitoring

CCTV monitors the school buildings on a continuous basis. CCTV monitors school minibuses whilst they are in use.

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.

Live images are not routinely monitored. Recorded footage is reviewed by authorised personnel only where there is a specific reason to do so, such as a reported incident, a safeguarding concern or a request from the police. The operation of the system, including image quality, camera positioning and the correct functioning of automatic deletion, is checked by authorised personnel at least termly, and that check is recorded.

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.

Signage and access to images

Where CCTV cameras are placed anywhere on the school site or in a school vehicle, 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. Recorded images will only be viewed in designated, secure offices.

5. Data and Image Retention

Images and recording logs must be retained and disposed of in accordance with the Data Protection Policy / Data Retention Schedule. Save where one of the exceptions in section 6 applies, recorded images are automatically overwritten and permanently deleted 30 days after recording. 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. Any provider which installs, maintains, hosts or otherwise has access to our CCTV system acts as a data processor on our behalf, and we will put in place a written contract with each such provider containing the terms required by Article 28 UK GDPR.

6. Retention and erasure of data gathered by CCTV

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.

Where footage relates to, or forms part of, a safeguarding or child protection concern, it will be downloaded before the automatic deletion period expires and retained on the relevant child protection file in accordance with our Child Protection and Safeguarding Policy and the retention periods that apply to safeguarding records, rather than the period set out in section 5. Where footage is or may be relevant to a police investigation, disciplinary process, insurance claim or legal proceedings, it will similarly be preserved for as long as necessary for that purpose.

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.

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 whether they are appropriate and will carry out a data protection 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.

Lockers Park 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. In this situation we 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.

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 (including the completion of a DPIA), 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 Headmaster, who will first take advice from the Data Protection Lead and, where any pupil may be affected, from the Designated Safeguarding Lead. 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. The Headmaster will have regard to the completed DPIA when making that decision. The School is not a public authority able to authorise directed surveillance under the Regulation of Investigatory Powers Act 2000; where conduct of that kind appears to be necessary, the matter will be referred to the police rather than undertaken by the School.

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

No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Headmaster (or, in the Headmaster's absence, the Deputy Head). 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.

Requests from parents to view footage of an incident involving their child will be considered on a case-by-case basis by the Data Protection Lead. Where footage shows other identifiable children, it will not normally be released; we may instead offer a supervised viewing on school premises, or provide a written account of what the footage shows.

10. Subject access requests

Data subjects, including staff, 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 and the relevant privacy notice (the Staff Privacy Notice, or the Pupil and Parent Privacy Notice) and it will be handled in line with data protection law and Lockers Park 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).

Where we reasonably require further information in order to identify the footage requested, we may ask the requester for clarification. In that event, and in accordance with Article 12A UK GDPR, the period for responding does not run while we are waiting for that clarification. We will not seek clarification as a matter of routine, and will do so only where it is reasonably required in order to respond.

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. We may also offer for you to view the footage on school premises if appropriate.

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.

When we respond to a subject access request we will also tell the requester of their right to make a complaint to the School under section 164A of the DPA 2018 (see section 12) and of their right to complain to the Information Commissioner.

11. Requests to prevent processing

We 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 the Staff Privacy Notice and the Pupil and Parent Privacy Notice. For further information regarding this, please contact the Data Protection Lead.

12. Complaints

Anyone — including a pupil, a parent, a member of staff or a visitor — who considers that the School has handled their personal data in a way that infringes data protection law may make a data protection complaint to the School. This right is given by section 164A of the Data Protection Act 2018.

A complaint may be made in any of the following ways:

in writing to the Data Protection Lead, Gavin Taylor, at headmaster@lockerspark.co.uk;

by post to the Data Protection Lead, Lockers Park School, Lockers Park Lane, Hemel Hempstead, Hertfordshire HP1 1TL; or

verbally, in person or by telephone, to the Data Protection Lead or to any member of the Senior Leadership Team, who will record it and pass it on.

A complaint does not have to be made on a particular form or use particular wording, and we will accept and act on a data protection complaint however it reaches us.

On receiving a data protection complaint we will:

acknowledge it in writing within 30 days of receipt;

make appropriate enquiries into the subject matter of the complaint;

keep the complainant informed of progress; and

tell the complainant the outcome of the complaint, and the reasons for it, without undue delay.

We keep a written record of every data protection complaint received, the steps taken in response, and the outcome.

Making a data protection complaint to the School does not remove the right to complain to the Information Commissioner, and a complainant may do so at any time. However, the Information Commissioner encourages individuals to raise the matter with us first. Details of how to contact the Information Commissioner can be found at www.ico.org.uk.

A member of staff who wishes to raise a concern about the use of CCTV that is not a complaint about the handling of their own personal data should speak to the Data Protection Lead in the first instance and, if the matter cannot be resolved informally, may use Lockers Park's formal Grievance Procedure (available within the Staff Handbook).

13. 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 Lead.