# Surveillance Management Procedure

**Contents**

## 1. Introduction

This procedure covers all matters relating to the use of video and audio recording equipment for overt surveillance in all buildings where our employees work, and which members of the public utilise. Examples of surveillance used in schools might include Closed Circuit Television (CCTV), Automated Numberplate Recognition (ANPR), drones, video doorbells and body worn cameras (BWC).

Covert surveillance under the Investigatory Powers Act (2016) is not covered by this document.

## 2. Quick Reference Guide

- Before undertaking surveillance complete a Data Protection Impact Assessment (DPIA) and consider if there is any other, less intrusive way, to meet your objective
- Always complete an impact assessment prior before siting cameras or other surveillance equipment to carry out any surveillance activity and consider whether you need to consult with those affected by the surveillance, or their parent/carers
- Ensure your privacy notices include details of any surveillance activities
- Ensure there is clear signage to make individuals aware that surveillance is in operation to comply with regulatory requirements
- Ensure all surveillance recordings are held securely with access controlled
- Ensure you have a process in place to enable access to surveillance recordings by individuals or investigators
- Do not keep surveillance data for longer than is necessary, and only retain in line with your retention policy
- Ensure relevant staff are trained to understand their responsibilities in relation to surveillance equipment and footage.

## 3. Policy References

This procedure is a requirement of the Data Protection Policy.

## 4. Surveillance Management Procedures

### Responsibility

Within the school responsibility for monitoring Data Protection issues resides with the Data Protection Officer (DPO). Responsibility for approving and reviewing this policy rests with the DPO. Responsibility for implementation of these procedures and for reporting performance issues under the policy rests with the Data Protection Lead and all employees who have involvement in the management of equipment. Responsibility for managing the deployment and use of cameras rests with your Senior Information Risk Owner (SIRO).

**Data Protection Impact Assessment**: Any use of surveillance must comply with the Data Protection Act 2018 and UK GDPR. Before any surveillance can take place a DPIA must be completed. This must identify the article 6 and 9 legal conditions you

 

will rely on for this processing. It must also consider whether your objective can be achieved through a less intrusive method. It will take into account other relevant legislation, for example Protection of Freedoms Act 2012, and the Human Rights Act 1998. Any surveillance equipment and footage storage must have appropriate security applied. Footage must only be retained for a limited period and be easily available whilst held should a request for access be made.

**Impact Assessments**

**Scope and Review**: The siting of each CCTV camera or other surveillance equipment that falls within the scope of this policy will be subject to an Impact Assessment (Annex A) before it is commissioned or a retrospective Impact Assessment where it was already operational before policy and this procedure was approved. Each site will be subject to a review against the Impact Assessment criteria every year, or sooner should there be any relevant change to the building use or a change in legislation. A register of surveillance equipment must be maintained (Annex B).

**Ownership**: Each site will have an identified owner who will take responsibility for the operation of all surveillance equipment on that premises or location. Accountability sits with the school as Data Controller. Where premises are shared with another organisation and control of surveillance equipment does not rest with the school, or where operation of equipment is contracted out to a service provider, the Impact Assessment will still record the organisation's Data Protection Lead as a point of contact who will be able to redirect queries to the relevant person outside of the organisation.

**Purpose**: The Impact Assessment will establish whether or not there is a need for surveillance in the first instance by recording the aims and benefits that the surveillance is meant to deliver and assessing whether there is any other, less intrusive, solution that could achieve this.

**Quality**: The level of detail required of surveillance recordings will vary according to the level of detail that is required for cameras to meet their stated purpose. For example, surveillance equipment used for recognition or identification will need better quality than those used for general monitoring. For footage to be admissible as evidence it must be of sufficient quality. Date and time stamp must also be regularly checked for accuracy.

**Wider Use:** Consideration will be given as to whether or not there is any wider use that surveillance serves other than the stated purpose. If there is then communicating this additional purpose in privacy information will be considered.

**Feedback:** Signage and explanatory publications will make site users aware of the purpose of the cameras and how to register feedback. Any complaints or concerns raised about the siting or usage of cameras will be captured and considered in a review. The outcomes of reviews will be communicated to those who have raised concerns, and to a wider audience if deemed appropriate

**Signage & explanatory publications**
**Signage.** Signs explaining that surveillance is operational in the vicinity shall be clearly visible and legible in accessible areas of the building. They will state:

- The name of the Data Controller
- The purpose of the processing
- How to access the full privacy notice (QR code or web address)

A sign template is available for your use at Annex E

**Retention, Security & Access**
**Retention of Recordings.** Our organisation commits to retaining recordings for security from surveillance cameras under its control for [31 days]. Cameras managed by partner organisations (not contracted service providers) are responsible for defining and publicising their own retention timescales. This period of time is based on the recommended range of 12-31 days and our experience of the need for authorised usage. When this time period has expired, the data on the recorded tape or server will either be recorded-over, degaussed (deleting magnetic storage content) or disposed of – in any event deleted beyond the ability to reconstitute the content.

**Security:** Once a recording is complete, the tape or other storage medium will be held in a secure container or on a secure server to which only authorised persons trained specifically in the policy and procedures have access.

**Access:** Instances of access to recordings will be recorded in a log which can be produced on demand to the DPO, an authorised manager, or Auditor/ Regulator and will be a complete record of access activity (Annex C). This log should state:

- Dates of access,
- the period and location covered by the recording,
- the reason for access and
- Name, position and authority of those who have accessed recordings.
- Whether or not copies were made.

**Usage**
**Our organisation's Usage:** We will only use recorded surveillance images for the purposes which we have identified in our Impact Assessments and communicated through signage and privacy information. A form is available for staff who need to carry out internal investigations (Annex D).

**Usage by other (third party) organisations:** We will ensure that where recordings are accessed by, or copies are provided to, other organisations this will also fall within these stated purposes, or otherwise within the law. Where copies are provided, the organisation requesting the material will be required to agree to manage the data in accordance with the Data Protection Act/ UK GDPR (Annex D). Where regular general information sharing with a partner takes place we will have in place an Information Sharing Protocol/Data Sharing Agreement.

**Recording:** Where use is made of recordings by us or access granted or copies provided to other organisations, these instances will be recorded and kept up to date in a central log available for inspection by anyone with the authority to monitor compliance with this policy. The reasons for use will be recorded and approved (Annex C).

## Handling Access Requests

**Rights.** Employees and members of the public whose images are captured by surveillance equipment have a right in law to access such recordings.

**Data Protection Law – Data Subject Access**

The Data Protection Act 2018 and the UK GDPR provide statutory rights for individuals (employees and members of the public) to have access to information held by organisations about themselves. By the very nature of surveillance images there is likely to be information present on recordings that identifies not just the requesting Data Subject but other persons who had been present. This will require an assessment of whether or not third parties can be identified and if so what method and level of redaction may be necessary. These requests are subject to a one-month statutory timeframe. Please see F3. SAR Procedure for more guidance.

**Data Protection Law – Crime & Taxation (S 2.1.2)**

Schedule Two, Part 1, section 2 of the Data Protection Act 2018 allows organisations to share footage with investigators for the purposes of crime prevention, detection and prosecution without the knowledge and consent of the data subject where to do so would prejudice the investigation. However, you must document the request and your response, and when making a decision regarding disclosure you must consider and record your rationale for the sharing; including the necessity, the proportionality of what has been requested, and your justification for doing so. Even if you do not disclose data, any such request must be logged.

**Freedom of Information Act.** The Freedom of Information Act provides general statutory rights of access to information held by Public Authorities. In practice, the rules governing this access regime will be applied where a requestor is asking for information about a person or persons other than themselves.

**Handling a Request.** Employees and members of the public will see signage and explanatory guidance at the locations where recordings are made that directs them to the appropriate contact to receive formal requests. Such requests should be directed to the school office.

## Equipment not managed by the school

**Shared or leased premises.** There may be instances of buildings where our employees are based where surveillance equipment is not directly controlled by us. Some of these buildings may be used by the public to access our services. Any equipment present in such circumstances is not managed by us and responsibility under Data Protection law therefore falls to the organisation in charge as they are the Data Controller. Such organisations should have in place the same provisions as described in this document including basic signage providing a contact point for queries and access requests. We have a responsibility to have appointed employees who will have limited responsibility for or oversight of the building and who are aware

of the partner organisation's provisions for surveillance recordings and can redirect enquires to the appropriate contact.

**Security Contractors.** Private companies may undertake surveillance recording and data handling on our behalf. Where this occurs, we have a responsibility to ensure that personal data is being managed according to the provisions in this policy or where there is any difference in practice, this is recorded, explained, noted in the policy and is within the law.

### 4.1 Closed Circuit Television (CCTV)

Any use of CCTV must conform to the following regulatory guidance How can we comply with the data protection principles when using surveillance systems? | ICO and Home Office Surveillance Camera Code. The following must be in place:

- A current DPIA and Impact Assessment
- Clear signage and a privacy notice online
- Staff training
- Footage quality and accuracy checks are regularly completed
- Date/time stamps are monitored and updated as required, for example changes between British summer and winter time
- Documented records management including security, retention and access
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request
- If CCTV can record audio, this should be switched off by default (see section 4.2)

### 4.2 Audio recording

You should not normally use surveillance systems to directly record conversations between members of the public. This is highly intrusive and unlikely to be justifiable in most circumstances. In most situations, the use of audio recording, particularly where it is continuous, is considered more privacy intrusive than purely visual recording. Its use will therefore require a much greater justification, and you should switch off by default any capability to record audio. You should only use it in exceptional circumstances, for example by a trigger switch.

If your system comes equipped with an independent sound recording facility, then you should turn this off or disable it in some other way, unless you can clearly justify and evidence its use. If you cannot control sound recording separately you need to consider how privacy intrusive the system is as a whole, including the recording of sound.

You should **only** use audio recordings when you have:

- identified a particular need or issue and can evidence that this need must be addressed by audio recording
- considered other less privacy intrusive methods of achieving this need

- reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is through the use of audio recording.

You should take additional steps to make it clear to individuals that audio recording is taking place, over and above any visual recording which is already occurring.

**4.3 Unmanned Ariel Systems (UAS/Drones)**
The use of Drones is only permitted where it is necessary, and then only if the operator has a flyer ID, the drone is registered with our operator ID and you fully comply with the requirements of the Unmanned Aircraft Systems (UAS) Regulations (Drone and Model Aircraft Code). The following must be in place:

- A current DPIA
- Clear signage and a privacy notice online
- Staff training
- Documented records management including retention and access
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request
- Registration with Civil Aviation Authority (CAA)

**4.4 Body Worn Video (BWV)**
Any use of BWV surveillance must conform to the following regulatory guidance - Body Worn Videos. The following must be in place:

- A current DPIA and Impact Assessment
- Clear signage and a privacy notice online
- Staff training
- Documented records management including retention and access
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request

**4.5 Surveillance in Vehicles**
Any use of vehicle surveillance (dashcams) must conform to the following regulatory guidance - Surveillance in Vehicles. The following must be in place:

- A current DPIA
- Clear signage and a privacy notice online
- Audio recording is switched off by default and only used in exceptional circumstances as defined by the Surveillance Lead
- Staff training
- Documented records management including security, retention and access
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request

**4.6 Action Cameras and other portable surveillance**
Any use of action cameras and other portable surveillance must conform to the following regulatory guidance - Action cameras and other portable surveillance

The following must be in place:

- A current DPIA and Impact Assessment
- Clear signage or announcements, and a privacy notice online
- Staff training
- Documented records management including security, retention and access
- The ability to redact footage (blur/mask/crop) to protect privacy in the event of an access request

**4.7 Facial Recognition technologies and surveillance**

Any use of facial recognition technologies and surveillance must conform to the following regulatory guidance - Facial Recognition technologies and surveillance
The following must be in place:

- A current DPIA is in place and an equalities impact assessment has been completed (EIA)
- A justification for the use of facial recognition is documented and kept under review
- Sufficient volume and variety of training data has been used to assure accurate performance
- A process is in place to identify false matches and true matches, and false positives can be recorded
- The system can be amended where false negatives or positives are too high
- Any watch lists comply with data protection law
- Staff training
- Documented records management including security, retention and access
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request

**4.8 Automatic Number Plate Recognition (ANPR)**

Any use of ANPR must conform to the following regulatory guidance - Automatic Number Plate Recognition and Home Office Guidance on ANPR Performance Assessment and Optimisation. The following must be in place:

- A current DPIA
- Clear signage and a privacy notice online
- Staff training
- Documented records management including security, retention and access
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request

**4.9 Smart Doorbells**

Any use of smart doorbells must conform to the following regulatory guidance – Smart Doorbells. The following must be in place:

- A current DPIA and Impact Assessment
- Clear signage and a privacy notice online
- Staff training
- Documented records management including security, retention and access

- Continuous recording is limited so the camera is only active when the doorbell is pressed
- The ability to redact footage (blur/mask) to protect privacy in the event of an access request

## 5. Parents who want to record meetings

Legally speaking, there is not a lot you can do if a parent wants to make an audio recording of a meeting. If the recording is for their personal use, they don't need to obtain consent or let other participants know.

Allowing parents to record a meeting is not necessarily a negative thing. It can work to safeguard the school, as parents will not be able to accuse the staff of saying something that they did not; having an exact record of something that went on, means there can be no misinterpretation of the conversation, so it could work to your advantage

Sometimes parents will record a meeting without your knowledge. Under the Regulation of Investigatory Powers Act 2000 (RIPA), it is not a criminal offence for a private citizen to make a recording in secret provided it is for personal use only. However, if the recording is then shared without consent of the participants, sold to a third party, or released in the public domain without the consent of the participants, this might then become a criminal offence.

## 6. Advice and Support

If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact the school office.

## 7. Breach Statement

A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

## Annex A: Surveillance Equipment Impact Assessment Forms

Surveillance Impact Asessment Form

## Annex B: Surveillance Equipment Register

Surveillance Equipment Register

## Annex C: Recordings Access Log

Surveillance Access Log

## Annex D: Subject Access Request Forms

### Data Subjects:

Data Subject Surveillance Access Fc

### Investigators (e.g. The Police):

S212 Access Request Form

### Internal investigations:

Surveillance Recordings Access r

## Annex E: Signage Template

CCTV poster.docx