Staffordshire University Academies Trust

CCTV Policy

Last reviewed	July 2024
Reviewed by	Operations Director
Approved by	Internally – CEO and DPO
Date of approval	July 2024
Policy owner	Operations Director
Location	Website

Purpose
The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) systems at the academies within Staffordshire University Academies Trust (SUAT). This policy details the procedures to be followed to ensure that the Trust and its academies comply with relevant legislation and codes of practice for processing data captured through use of CCTV systems, including that:

- We comply with the UK GDPR.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

We take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our estate and its members.

This policy will be subject to review annually to include consultation as appropriate with relevant parties, and has been compiled with regard to the Surveillance Camera Code of Practice and Information Commissioner's Office guidance for the use of video surveillance including CCTV – https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/

This guidance advises:

Building public trust and confidence is essential to ensuring that the benefits of any new technology can be realised. The public must have confidence that the use of surveillance systems is lawful, fair, transparent and meets the other standards set in data protection law.

S29(6) of the Protection of Freedoms Act 2012 (PoFA) states that "surveillance camera systems" mean:

(a) closed circuit television or automatic number plate recognition systems,

(b) any other systems for recording or viewing visual images for surveillance purposes,

(c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or

(d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

This policy has due regard to relevant legislation, statutory and non statutory guidance including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004

- Equality Act 2010
- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Video Surveillance'
- DfE (2022) 'Protection of biometric data of children in schools and colleges

1. Objectives of the CCTV Policy

- To increase personal safety of staff, pupils/students and visitors and reduce the fear of crime;
- To protect SUAT buildings and their assets;
- To support the police in a bid to deter and detect crime;
- To assist in identifying, apprehending and prosecuting offenders;
- To assist in managing the academies and the investigation of suspected breaches of Academy/Trust regulation;
- To help ensure that those capturing individuals' information comply with the DPA 2018, UK GDPR and other such relevant statutory obligations;
- To contribute to the efficient deployment and operation of a camera system;
- To ensure that the information captured is usable and can meet its objectives in practice;
- To reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- To re-assure those whose information is being captured, of Academy compliance;
- To manage the risks of using CCTV systems to capture personal information.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing.
- Taking action to prevent or detect a crime, damage to properties, violence or aggression towards premises occupants.
- Using images of individuals that could affect their privacy.

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

2. Statement of intent

Surveillance camera systems are deployed extensively within the UK and where they are used appropriately, these systems are valuable tools which contribute to public safety and security and in protecting both people and property. The Trust and its academies seek to operate CCTV systems in a manner that is consistent with respect for the individual's privacy.

The majority of surveillance systems are used to monitor and/or record the activities of individuals and as such they process individuals' personal data. Academy use of surveillance systems will therefore be covered by the Data Protection Act 2018 and the UK GDPR, and the provisions of the ICO's codes of practice for the use of CCTV systems and surveillance.

The accountability principle requires academies using CCTV systems to take responsibility the processing activities that are undertaken with personal data, and compliance with the principles of data protection, designated under the UK GDPR. Academies using CCTV are required to have appropriate measures and records in place to be able to demonstrate compliance. Accountability obligations are maintained throughout the life of the processing.

Using surveillance systems can be privacy intrusive. They are capable of placing large numbers of law abiding people under surveillance and recording their movements as they go about their day to day activities. As such, academies will carefully consider whether or not to use a surveillance system and will take into account the nature of the problem they are seeking to address, inclusive of:

- Whether a surveillance system would be a justified and effective solution
- Whether better solutions exist
- What effect its use may have on individuals, and whether in the light of this, its use is a proportionate response to the problem

As such, SUAT and the academies will treat the systems and all information, documents and recordings obtained and processed as data which are governed by the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). Cameras will be used to monitor activities within Academy premises; buildings, car parks and other such public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of ensuring the safety and wellbeing of Academy staff, pupils/students and visitors, alongside the security of the premises. It is likely that the majority of use of CCTV systems will be under the GDPR's lawful basis for processing – Public Task - Article 6(1)(e).

All planning and design has and will endeavour to ensure that the CCTV systems being used, will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

The use of CCTV systems in academies will be regularly reviewed for effectiveness in accordance with their original purpose for siting. Cameras in situ will be subject to review at least on an annual basis. CCTV which is not utilised for its original purpose in accordance with section one of this policy, or which is no longer effective, may be subject to decommission following reviews of usage.

It should be noted that CCTV is not utilised in all SUAT Academy buildings and external premises and therefore this policy only applies to those academies who operate CCTV systems.

For the purpose of this policy the following definitions are given for the below terms:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The Trust does not condone the use of covert surveillance when monitoring staff, pupils and others occupying the premises. Covert surveillance will only be operable in extreme circumstances.

- **Biometric data** – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition.

- **Automated biometric recognition system** – a system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically'.
- **Facial recognition** – the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template.

3. Operation of the System

3.1 This policy will be administered and managed by the Principals / Head Teachers or their nominee, in accordance with the principles and objectives expressed in this policy and the relevant data protection laws. The day-to-day management will be the responsibility of the Leadership Teams (SLT), ICT Technicians and the Premises Managers. The CCTV system is capable of being operated for 24 hours per day, every day of the year. Surveillance will be used as a deterrent for violent behaviour and damage to academies. Surveillance is conducted as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in classrooms or any changing facility.

3.2 Systems in place comprise of a number of fixed cameras located around Academy premises where there is a legitimate requirement for such monitoring in accordance with the purpose limitation principle of the UK GDPR; 'personal data should be collected for specific and legitimate purposes and must not be further processed in a way which is incompatible with such purposes.'

3.3 In accordance with the Surveillance Camera Code of Practice, CCTV System operators should adopt the following guiding principles:

- *Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.*
- *The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.*
- *There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints, this will usually be via the Academy's privacy notices.*
- *There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.*
- *Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.*
- *No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.*
- *Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.*
- *Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.*
- *Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use, both physically and technically.*
- *There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.*
- *When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.*

- *Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.*

3.4 Camera footage can **only** be reviewed and managed by designated staff (Academy employed IT Technicians and Network Managers, Premise Managers and Senior Leadership Teams) in accordance with the integrity and confidentiality principle of the UK GDPR, to ensure that all personal data is maintained on a confidential basis, is secure against unlawful processing, accidental loss or disclosure, destruction or damage.

3.5 The CCTV systems will be used to observe Academy premises and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident.

3.6 Staff are instructed that static cameras are not to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the Academy's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

3.7 Classroom footage will not be used for the purposes of staff Performance Management, capability or disciplinary action. CCTV will only be used for the objectives outlined in section one of this policy.

3.8 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Footage will only be released to the media for use in the investigation of a specific crime and with the written authority of the police and following consultation with the CEO, DPO and ICO as necessary to conform with the principles of data protection in accordance with the UK General Data Protection Regulation and Data Protection Act 2018. Footage will never be released to the media for purposes of entertainment. Compliance with the UK GDPR will be maintained for use of CCTV systems.

3.9 Each Academy that houses CCTV must have a map of the locations of each camera installation, to support in monitoring and reviewing the purpose of each sited camera. The system should be maintained to permit optimum performance and address functionality issues.

3.10 Signs notifying premise users of the presence of CCTV, as required by the Code of Practice of the Information Commissioner must be placed at all access routes to areas covered by CCTV. Processing in a transparent manner means that people are informed when their data is being captured.

3.11 Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with SUAT policies and procedures and be authorised by the CEO and ICO.

3.12 Specific purposes for the processing of personal data and use of CCTV information must be defined and communicated to those operating the systems. Data must be processed lawfully, fairly, and in a manner that people would reasonably expect, taking into account advancements in technology that may not be anticipated by some people.

3.13 There must be clearly defined procedures in each setting, regarding how data will be managed in practice, authorised users of CCTV systems, security measures surrounding CCTV systems etc. Data will not be shared without a designated purpose, in keeping with the principles of data protection, and with approval from the DPO and CEO.

3.14 A Data Protection Impact Assessment should be compiled for the use of CCTV systems, as outlined within this policy document. Any new CCTV system or additional cameras being installed to an existing system must be subject to a data protection impact assessment. DPIAs must: describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance

measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. Screening checklists can also be completed to help inform the DPIA - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

3.15 The information the surveillance system processes must be of good quality and be adequate, relevant and limited to what is necessary. Academies must identify the minimum amount of personal data they need to fulfil their purpose(s) for processing the data.

3.16 Both fixed and mobile cameras must be focussed on a relevant space, and where wider surveillance is possible but unnecessary, this should be restricted. This ensures that surveillance does not occur in areas which are not of interest and individuals are not unintentionally made the subject of surveillance.

3.17 Academies will not use biometric CCTV systems or systems which can be used to record audio.

3.18 The data must be collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:

- Further processing for archiving data in the public interest
- Scientific or historical research
- Statistical purposes

3.19 Those under surveillance should clearly be aware that they are being recorded. Academies should provide individuals with appropriate information about how they can exercise their rights, and that appropriate restrictions on viewing and disclosing images are in place for those using the system. In SUAT academies, this would usually be provided through signage and privacy notices. It is important that signs are placed prominently before the entrance to the system's field of vision and for this to be reinforced with further signs inside the area. Information should be positioned at a reasonable distance from the places monitored, and in such a way that individuals can easily recognise the circumstances of the surveillance before entering the monitored area.

Where processing is not obvious to an individual, a sign could read "Images are being monitored and recorded for the purposes of crime prevention and public safety. This system is controlled by XXXXX. For more information, visit our website at (web address) or call XXXXXX."

3.20 The reasons for selecting a particular surveillance system should not be based solely on technical capabilities, including the quality of the images it can produce, the field of vision it offers or the amount of data it can record. Academies must also consider the governance capabilities that complement the system, such as software that enables footage to be uploaded, stored and audited. Personal data should be easily retrievable in response to a subject access request and other individual rights. Academies should ensure that your systems have the capability to redact footage if third parties need to be blurred or obscured.

3.21 Data collected from CCTV should be accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

3.22 Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

3.23 Data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.24 Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

3.25 Academies using CCTV should ensure that their signage is compliant by:

- Ensuring that signage is clear and visible, e.g. outdoor signs are not covered by overhanging branches.
- Ensuring that signage is an appropriate size, e.g. if the CCTV is located near a drop off point it needs to be big enough for driver to see it from inside a car.
- Ensuring that, if it captures images outside the Academy site, signs are clearly displayed for pedestrians.
- Ensuring that staff know who to talk to if they get asked about the images captured on CCTV.[1]

Furthermore, when creating CCTV in operation signs, the wording used must include:

- The details of the organisation operating the system.
- The purpose of its use, e.g. crime prevention.
- Who to contact if individuals have any enquires pertaining to the images being captured by the CCTV.

4. Monitoring procedures

4.1 CCTV images will not be continuously monitored. Where staff are not monitoring the system, the system should be locked or made otherwise inaccessible to unauthorised personnel. CCTV must not be controlled by unauthorised personnel and screens used to view footage must not be accessible or viewable by those who do not have authorisation to do so.

4.2 Recorded images must be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to authorised persons as mentioned in section one of this document. Where images are in an area of particular sensitivity, it may be more appropriate to only view recorded images after an incident has occurred.

4.3 CCTV should only be accessible through password protected and suitably encrypted devices. Passwords must be changed on at least a termly basis, be of suitable length and with a variety of characters and numbers, i.e. at least eight characters of upper and lower case and at least one number.

4.4 Images are recorded on servers located securely in each Academy. Server rooms must be secure and accessible only to authorised members of staff. Additional staff may be authorised by the Principal / Head Teacher to temporarily monitor cameras sited within their own areas of responsibility, provided that the footage is viewed purely for the purposes defined within this policy and on a view only basis. All staff must adhere to the code of conduct and maintain strict confidentiality when viewing CCTV.

4.5 Server rooms and the facilities/assets contained within them will be subject to regular maintenance by external contractors. Academies must ensure that CCTV systems are appropriately locked and secure to ensure that the information within these systems remains inaccessible to unauthorised parties, and that contractors are inducted to site security accordingly to ensure that they are aware of their obligations to ensure system security and confidentiality is maintained.

4.6 Cameras are monitored in designated rooms, circulations and external areas, which differ at each Academy, but are a secure area and staffed during working hours. Damage is reported to appropriate staff. The cameras installed must provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked and maintained at regular intervals to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

4.7 When implementing appropriate technical and organisational security measures, Academies must ensure that:

- Any ability to make copies of information is restricted to appropriate and approved staff;
- There are sufficient controls and safeguards in place if the system is connected to, or made available, across a network;
- Where information is disclosed to a third party, academies are able to safely deliver it to the intended recipient;
- Control rooms and rooms where information is stored are secure;
- Staff are trained in security procedures, with sanctions against staff who misuse surveillance system information;
- Staff are aware that they could be committing a criminal offence if they misuse surveillance system information;
- There are any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied to the system or any other devices connected to it, or both.

4.8 Academies should build in a periodic review of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, academies should stop the processing until they can modify the system accordingly. Systems should be checked for functionality and placement on a monthly basis, with an annual formal recorded review in conjunction with the DPO.

4.9 All checks should ensure that data being collected is accurate; not excessive; used only for defined purposes; and that the use is still necessary and proportionate throughout the lifecycle of the processing.

4.10 CCTV systems should be tested for security flaws half termly to ensure that they are being properly maintained at all times. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

4.11 The ability to produce copies of information will be limited to the appropriate staff approved by the Headteacher and DPO.

4.12 Any unnecessary footage captured will be securely deleted from the system.

4.13 All images recorded by the CCTV System remain the property and copyright of the Trust, and CCTV systems themselves are owned by the Trust. The monitoring of staff, pupil/student and visitor activities will be carried out in accordance with Trust policies and practices.

4.14 To comply with the requirements of the Protection of Freedoms Act 2012, academies will notify all parents of its intention to process pupils' biometric data and emphasise that parents may object at any time to the processing of the information. The processing of biometric information will not be undertaken without the approval of the DPO and completion of a DPIA.

4.15 Academies will ensure that pupils' biometric data is not taken or used as part of a biometric recognition system if pupils under the age of 18 object or refuse to participate in activities that involve the processing of their biometric data. A pupil's objection or refusal overrides any parental consent to the processing of data. Academies will ensure that information is included in its privacy notices that explains how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing. Reasonable alternative arrangements will be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent or due to

the pupil's own refusal to participate in the collection of their biometric data. The alternative arrangements will ensure that pupils do not suffer any disadvantage or difficulty in accessing services and premises. Likewise, such arrangements will not place any additional burden on parents whose children are not participating in such a system.

5. Installation of New Systems and the Addition of Cameras

5.1 Any proposed new CCTV installation is subject to a Data Protection Impact Assessment and must be able to demonstrate a clear purpose to protect the Academy building(s) and/or occupants.
5.2 Any proposed additions to existing CCTV installations are subject to a Data Protection Impact Assessment and must be able to demonstrate a clear purpose to protect the Academy building(s) and/or occupants.
5.3 Consultation with the DPO is required for new installations and the addition of cameras and will be subject to approval by the DPO and CEO.

6. Review of System Usage

6.1 The use of each CCTV system should be reviewed on at least an annual basis for effectiveness and to ensure that the system fulfils the purpose for which it was originally installed.
6.2 Appendix B of this policy should be utilised to perform the review.
6.3 The siting of each camera on the system must be reviewed, alongside the system as a whole.
6.4 Cameras which are deemed ineffective or can no longer be utilised for the purposes they were original installed will be decommissioned accordingly.

7. Compliance with Data Protection Legislation

In administration of CCTV systems, Academies must ensure that they comply with the UK GDPR and follow Trust policies for Data Protection and Compliant Records Management. The principles of the UK GDPR define that personal data shall be;

- Processed lawfully, fairly and transparently;
- Collected for specific, explicit and legitimate purposes in accordance with the purpose limitation principle;
- Limited in processing to what is necessary to fulfil the purpose for which it was collected
- Accurate;
- Kept in a form which permits identification of data subjects for no longer than is necessary to fulfil processing purposes;
- Subject to appropriate security measures, including protection against unauthorised or unlawful processing against accidental loss, destruction or damage, using suitable organisational measures in order to meet the principle of confidentiality and integrity;
- Maintained in accordance with the accountability principle. Academies utilising CCTV maintain the responsibility for ensuring compliance with data protection laws.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Any and all uses of CCTV systems must be in accordance with relevant data protection legislation; Academies and their staff who utilise such systems must protect the personal data contained both in electronic storage systems and through live footage by:

- Keeping the data in a form which identifies individuals for no longer than the specified retention period unless there are compelling legal reasons to do so, such as the footage will be utilised as part of criminal proceedings in a court of law;

- Be used only to collect data for the purposes outlined in section one of this policy; mainly to safeguard staff, pupils and visitors on the premises from crime and to act as both a deterrent to crime and an aid in prosecution where the deterrent has not been successful;
- Informing individuals about the usage of CCTV on the premises through appropriate signage and privacy notices;
- Be positioned in places which comply with the purposes for which the cameras are being used;
- Regularly reviewing the effectiveness of the system, and the requirements for CCTV.

Changes in the use of systems must be reflected in Academy privacy notices.

8. Access by the Data Subject

8.1 The UK General Data Protection Regulation (Article 15) provides Data Subjects (individuals to whom "personal data" relate) with a right of access to data held about themselves, including those obtained by CCTV. Where a request for access is made, this is called a Subject Access Request (SAR). SARs must be made to the individual Academy's Data Protection Representative, as outlined in the privacy notices for each Academy. In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is classified as personal information about the individual concerned.

8.2 In order to locate images on the Academy's CCTV system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject found, defined as the scope of the request. Academies who receive a SAR of this nature must follow SUAT's procedure for handling Subject Access Requests and consult with the DPO prior to providing personal information. The Academy and DPO may consider that it would be more suitable for the individual to attend site to view the footage, rather than providing a copy.

8.3 Academies will protect the rights of third parties whose images may also be captured on the CCTV footage requested by obscuring their identity as far as reasonably practical. Where the Academy is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it must consult with the DPO prior to releasing any information. The Academy may not be obliged to comply with the request unless satisfied that the third party has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the third party or that reasonable measures can be taken to protect the identity of the individual, without having their consent for release of data as per the SAR. Consultation will be undertaken with the ICO as deemed necessary by the DPO in accordance with the request.

8.4 A request for images made by a third party (SAR) should be made in writing to the Data Protection Representative at each Academy. Data requested as part of a SAR will not be released until the Academy has satisfactorily verified the identity of the individual and followed the Subject Access Request procedure in consultation with the DPO. Data that can be released in compliance with the law, will be released within one calendar month of the request, or three calendar months where there are exceptional circumstances and an extension can compliantly be applied. The Academy must consider whether the data will be removed from the system before the SAR can be fulfilled, in order to preserve it e.g. the system holds CCTV data for one calendar month but the individual has made a request on day 15 and the Academy therefore needs to continue to hold the data through following the SAR procedure.

8.5 In limited circumstances, it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation. Such disclosures will be made in conjunction with the DPO and ICO (where relevant) with reference to applicable legislation and in accordance with this policy.

8.6 Academies may provide access to CCTV images to Investigating Officers when sought as evidence in relation to cases relating to staff, students/pupils or visitors, and where they have obtained the consent

of the individual in order to do so, where consent is required in accordance with the nature of the individual case. This is upon consultation with the DPO and approval of the CEO, with advice from HR providers and the ICO, depending on the nature of the case and data involved.

8.7 Academies must ensure that any disclosure of information to third parties from the surveillance system is controlled and that the disclosure itself is consistent with the purpose(s) for which the system was set up.

8.8 Academies should approach any requests for information with care, as wider disclosure may be unfair on the individuals concerned. Some disclosures to third parties may be unlawful and qualify as an offence under Section 170 DPA 2018 if the disclosure was made knowingly or recklessly without the consent of the controller. No CCTV footage will be placed on the internet.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure. Any copied CCTV footage will be subject to suitable encryption methods before being released.

8.9 Where copies of information are provided, this will be supplied to the individual free of charge; however, academies may impose a 'reasonable fee' to comply with requests for further copies of the same information. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

8.10 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

8.11 It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

9. Third party access

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

In order to maintain and preserve the integrity of the disks or other portable devices (such as USB drives or hard drives) used to record events, store data and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each disk/portable device containing personal identifiable information in the form of CCTV footage must be identified by a unique mark **and encrypted prior to release.**
- Before using each disk/portable device must be cleaned of any previous recording.
- The Academy shall register the date and time of the disk/portable device insert, including reference.

- A disk/portable device required for evidential purposes must be sealed, witnessed, signed by the Academy, dated and stored in a separate, secure, evidence disk store. If a disk/portable device is not copied (if required for copy) for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence disk/portable device store.
- If the disk/portable device is archived the reference must be noted, and the purpose for archiving must be recorded.
- Disks/portable devices containing footage may be viewed by the Police for the prevention and detection of crime and authorised officers of SUAT for supervisory purposes.
- A record will be maintained of the release of disks to the Police or other authorised applicants as part of the procedure for releasing data for a Subject Access Request. A register will be available in each Academy for this purpose.
- The viewing of disks/footage located on portable devices by the Police must be recorded in writing. Requests by the Police can only be actioned under requirements set out in the UK GDPR for authorised Subject Access Requests (see section 8 of this policy). Should a disk/portable device containing footage be required as evidence, a copy may be released to the Police under the procedures described in this policy. Disks/portable devices containing footage will only be released to the Police on the clear understanding that the disk remains the property of SUAT, and both the disk/portable device and information contained on it are to be treated in accordance with this policy. SUAT also retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon. On occasions when a Court requires the release of an original disk this will be produced from the secure evidence disk store, complete in its sealed bag. The Police may require the Academy to retain the stored disks for possible use as evidence in the future. Such disks will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. solicitors) to view or release disks will be referred to the Chief Executive Officer and Data Protection Officer. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.
- Disks are retained for the period in which they are required to fulfil the original purpose of the subject access request. They must then be returned to the Academy for appropriate disposal/deletion/retention in accordance with the SUAT Retention and Records Management Policy. The return of the disk/portable device must be logged in the document described in this policy.
- All requests for accessing personal data recorded on CCTV systems must be recorded on the electronic data protection system.

10. Right to Erasure

Article 17 of the UK GDPR provides individuals with the right to have personal data erased, however, the right is not absolute and only applies in certain circumstances. This could, for example, be a request from an individual to request erasure of unnecessarily retained CCTV footage.

This right can apply to CCTV footage if:

- The information is no longer necessary for the purpose which the Academy originally collected or processed it for;
- The Academy is relying on legitimate interests as the basis for processing, the individual objects to the processing of their information, and there is no overriding legitimate interest to continue this processing;
- The Academy has processed the personal information unlawfully (i.e. in breach of the lawfulness requirement); or

- The Academy to erase it to comply with a specific legal obligation.

There are circumstances where the right to erasure cannot be exercised as certain exemptions apply, and this may include but is not limited to:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- Certain research activities; or
- Compliance with a specific legal obligation to process surveillance information.

Requests for erasure should be referred to the DPO as soon as possible.

11. Restricting Processing

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances, meaning that an individual can limit the way that an Academy uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information the Academy holds or how it has processed their data. In most cases, academies will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time.

The UK GDPR suggests a number of different methods to restrict data usage, such as:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users; or
- Temporarily removing published data from a website.

12. Storage and Retention of Images

12.1 Personal data captured on CCTV footage will be retained and stored in accordance with the principles of the UK GDPR. Footage will be stored on the Academy's system for 30 days, unless retention is required for purposes outlined in this policy; as part of a Subject Access Request or where the Academy is required to submit or retain the data on a legal basis for law enforcement and regulatory purposes.

12.2 Recorded material must be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used where there is a legal basis to do so e.g. where it is permissible as evidence in court. Academies must consider the medium of storage and the footage must be encrypted; consultation with the DPO should be made to support the maintenance of adequate security measures. Academies must keep a record/audit trail of how the information is handled if it is likely to be used as evidence in court and once there is no reason to retain the recorded information, it should be deleted and the deletion of such data recorded.

12.3 Where data is stored, this shall be done so in accordance with the integrity and confidentiality principle of the UK GDPR, on a secure server which is appropriately protected from viruses and unauthorised access, and is located in a secure and lockable location, accessed by authorised personnel only. Authorised personnel includes certified security companies who maintain and support the use of the CCTV system.

12.4 Screens and monitoring systems which show the footage must be kept in a lockable room which is inaccessible to unauthorised personnel, and locked/inaccessible to unauthorised personnel when not in use.

12.5 Where footage is transferred to portable devices such as disks and USB drives for the purpose of responding to a Subject Access Request, these must be encrypted and used in accordance with this policy. The portable media must be purchased by the Academy and verified by IT Support providers as safe for use (and not subject to cyber security risks such as malware).

12.6 Footage must be retained in accordance with the SUAT Retention and Records Management Policy.

12.7 Any device used to access recordings must be subject to the appropriate security features, as detailed within the Information Security Policy. Devices must be encrypted, password protected and accessible only to authorised staff. Devices must be protected from unauthorised access and personal devices must not be used to access CCTV footage.

12.8 CCTV must not be subject to live monitoring.

13. Breaches of the Code (including breaches of security)

13.1 Any breach of the CCTV Policy and/or the CCTV Code of Practice by SUAT staff will be initially investigated by the Principal/Headteacher, in order for them to follow the designated human resources procedures. The DPO/CEO must be informed immediately.

13.2 Any breach of the Code of Practice which involves a possible breach of data protection legislation will be reported to the DPO in accordance with the SUAT Personal Data Breach Management Plan, who will support with the reporting of the personal data breach to the ICO within 72 hours of the detection of the breach. SUAT's personal data breach management plan will be consulted and followed.

13.3 An independent investigation will be carried out to make recommendations on how to remedy the breach. Findings of the Investigation must be reported to the CEO / DPO.

14. Assessment of the Policy

Performance monitoring, including random operating checks, may be carried out by the Chief Executive Officer and Data Protection Officer.

15. Complaints and Queries

15.1 Any complaints about SUAT's CCTV systems should be addressed to the Principal / Head Teacher of the relevant Academy in the first instance, or in the event of a complaint/concern in relation to personal data, this should be addressed to the Academy's Data Protection Representative as described in the Academy's Privacy Notice.

15.2 Complaints will be investigated in accordance with SUAT's Complaints Policy and Procedures, Data Protection Policy and Retention and Records Management Policy.

16. Communication

16.1 All staff involved in the operation of CCTV systems will be made aware of this policy and will only be authorised to use the CCTV system in a way that is consistent with the purposes and procedures contained therein. Staff will be trained in compliance procedures as well as the use of the system itself.

16.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images must ensure that they are compliant with SUAT's data protection policies.

16. Public information and Freedom of Information Requests

16.1 Copies of this policy will be available on the SUAT website.

16.2 Academies should have a member of staff who is responsible for responding to freedom of information requests and understands the Academy's responsibilities. They must respond within 20 working days from receipt of the request. Section 40 of the FOIA and section 38 of the FOISA contain a two-part exemption relating to information about individuals. If academies receive a request for surveillance system information, they are required to consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA and FOISA. Instead this request should be treated as a data protection subject access request as explained above.
- Is the information personal data of other people? If it is, then the information can only be disclosed if this would not breach the data protection principles. In practical terms, if individuals are capable of being identified from the relevant surveillance system, then it is personal information about the individual concerned. It is generally unlikely that this information can be disclosed in response to a freedom of information request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may be unfair processing in contravention of the DPA 2018 and UK GDPR.

The following conditions should be considered:

First condition: disclosure does not contravene one of the data protection principles.

Second condition: disclosure does not contravene an objection to processing.

Third condition: the information is not exempt from the right of access.

15.3 When deciding on whether disclosure is appropriate, academies can consider the expectations of the individuals involved, what the information considered for disclosure would reveal and the legitimate public interest in the information. Where academies think that obscuring images will appropriately anonymise third party personal data, i.e. it is reasonably likely that the requestor or anyone else can identify the individuals whose personal data you wish to protect (disclosure under FOIA being disclosure to the world), then it may be appropriate to do this rather than exempting the information. For example, requestors may ask for information regarding the operation of the systems, the siting of them, or the costs of using and maintaining them. If this information is held, then consideration will need to be given to whether or not it is appropriate to disclose this information under FOIA. If it is not appropriate to disclose this information then an exemption under FOIA will be used, if one is applicable.

15.4 Academies who receive a request for CCTV data under the FOIA must consult with the DPO before releasing the data and record this on the data protection system.

15.5. Academies may also receive requests for information under FOIA relating to those surveillance systems. For example, requestors may ask for information about the operation of the systems, the siting of them, or the costs of using and maintaining them.

If Academies hold this information, considerations as whether it is appropriate to disclose this information under FOIA must be made. Academies should provide any information you hold unless an exemption applies. For example, if providing details of the location of cameras is likely to prejudice the prevention or detection of crime.

16. Appendices

APPENDIX A
REGULATION OF INVESTIGATORY POWERS ACT 2000
PART II APPLICATION FOR AUTHORITY FOR DIRECTED SURVEILLANCE

APPENDIX B
REGULATION OF INVESTIGATORY POWERS ACT 2000
RECORD OF REVIEW

APPENDIX C
REGULATION OF INVESTIGATORY POWERS ACT 2000
PART II APPLICATION FOR RENEWAL OF DIRECTED SURVEILLANCE AUTHORITY

APPENDIX D

REGULATION OF INVESTIGATORY POWERS ACT 2000
PART II - CANCELLATION OF DIRECTED SURVEILLANCE

APPENDIX E
REGULATION OF INVESTIGATORY POWERS ACT 2000
CONCLUDING REPORT

APPENDIX F
SURVEILLANCE CAMERA CODE OF PRACTICE

Resources:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

APPENDIX A

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART II APPLICATION FOR AUTHORITY FOR DIRECTED SURVEILLANCE

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Full Address			
Contact Details			
Operation Name (if applicable)			

Details of application:

1. The level of authority required in accordance with the Regulation of Investigatory Powers Act 2000	
PRINCIPAL	

2. Grounds on which the action is <u>necessary</u>: *delete as inapplicable*
In the interests of national security;
For the purpose of preventing or detecting crime or of preventing disorder;
In the interests of the economic well-being of the United Kingdom;
In the interests of public safety;
For the purpose of protecting public health;
For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

3. Explain why the directed surveillance is proportionate to what it seeks to achieve

4. The identities, where known, of those to be subject of the directed surveillance:	
Name:	
Address:	
DOB:	

Other information as appropriate:	

5. The action to be authorised, including any premises or vehicles involved;
6. Give an account of the investigation or operation;

7. Explanation of the information which it is desired to obtain as a result of the authorisation:

8. Collateral Intrusion: INDICATE ANY POTENTIAL FOR COLLATERAL INTRUSION ON OTHER PERSONS THAN THOSE TARGETED: INCLUDE A PLAN TO MINIMISE COLLATERAL INTRUSION

9. Confidential/Religious Material: INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL/RELIGIOUS MATERIAL:

Anticipated Start	**Date:**		**Time:**	

10. Applicant's Details			
Name (print)		**Tel No:**	
Signature		**Date**	

11. Authorising Officer's Comments.

12. Authorising Officer's Recommendation.			
I, [ ], hereby authorise the directed surveillance operation as Detailed above. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).			
Name (Print)		**POSITION**	
Signature		**Date**	

13. Confidential Material Authorisation.			
Name (Print)		**POSITION**	
Signature		**Date:**	
From Time		**Date:**	

14. Urgent Authorisation: Details of why application is urgent.

Name (Print)		**POSITION**	
Signature		**Date/Time**	

15. Authorising Officers comments. (This must include why the authorising officer or the person entitled to act in their absence considered the case urgent).

16. Please give the reasons why the person entitled to act in urgent cases considered that it was not reasonably practicable for the authorisation to be considered by a person otherwise entitled to act.			
Name (Print)		**POSITION**	
Signature		**Date/Time**	

Appendix B

REGULATION OF INVESTIGATORY POWERS ACT 2000

RECORD OF REVIEW

Public Authority *(including full address)*	

Applicant		**Position Held**	
Operation Name		**Operation Number*** *Filing Ref	
Date Of Authorisation			

2. Detail any significant changes to the information in the original authorisation

3. Explain the continuing need for authority

4. Explain why the directed surveillance is still proportionate to what it seeks to achieve and in particular demonstrate that the degree of intrusion into the privacy of those affected by the surveillance in commensurate with the seriousness of the offence. In particular consideration should be given to: ***a) Proportionality*** *– the use of surveillance must be proportional to the problem it is intended to solve. Levels of intrusion must be appropriate to the severity of the matter under investigation – serious breaches of an individual's right to privacy can only be justified in operations concerning serious crime.* ***(b) Compulsion*** *– is the use of directed surveillance essential to the success of the operation or investigation. It must be demonstrated that other investigative methods either; have been tried without success, are not feasible, not sufficiently reliable or impractical to use in the context of the type of crime or general volume of activity.* ***c) Sufficiency of intrusion*** *– will be directed surveillance be tightly focused on the subject? Is the degree of collateral intrusion affecting individuals not connected with the investigation or operation justifiable and acceptable?*

5. Applicant's Details			
Name (Print)		**Tel No.**	
Position		**Date**	
Signature			

6. Authorising Officers Comments

7. Authorising Officer's Acknowledgment			
Name (Print)		**Position**	
Signature		**Date/Time**	

APPENDIX C

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART II APPLICATION FOR RENEWAL OF DIRECTED SURVEILLANCE AUTHORITY (Please attach the original authorisation)

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
		Renewal Number	

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail any significant changes to the information in the previous authorisation.

4. Detail why it is necessary to continue with the authorisation.

5. Indicate the content and value to the investigation of the product so far obtained by the surveillance.

6. Give an estimate of the length of time the authorisation will continue to be necessary.

7. Applicant's Details			
Name (Print)		**Position**	
Signature		**Date/Time**	
8. Authorising Officer's Comments.			

9. Authorising Officer's Recommendation.				
I, [ ], hereby authorise the directed surveillance operation as Detailed above. This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).				
Name (Print)			**POSITION**	
Signature			**Date**	
Renewal From	**Time:**		**Date:**	

APPENDIX D

REGULATION OF INVESTIGATORY POWERS ACT 2000

PART II - CANCELLATION OF DIRECTED SURVEILLANCE

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Operation Name		**Operation Number*** *Filing Ref	
		Renewal Number	

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Time and Date of when the authorising officer instructed the surveillance to cease.			
Date		**Time**	

4. Authorisation cancelled	**Date:**		**Time:**	

5. Authorising Officer's Recommendation.			
I, [ ], hereby authorise the cancellation of the directed surveillance operation as detailed above			
Name (Print)		**POSITION**	
Signature		**Date**	

APPENDIX E

REGULATION OF INVESTIGATORY POWERS ACT 2000

CONCLUDING REPORT

Establishment *(including full address)*			
Name of Applicant		**Position Held**	
Operation Name		**Operation Number*** *Filing Ref	
Date of Authorisation			

1. Concluding Review – The dates and a brief description of the nature of the surveillance conducted must be recorded in this grid at the conclusion of the authorised surveillance operation			
Date Surveillance undertaken	**Details of any intrusion into privacy of any person involved in or affected by the surveillance**	**Comments/Observations**	**Officer Reporting and date report made**

2. Applicant's Details			
Name (Print)		**Tel No.**	
Position		**Date/Time**	
Signature			

3. Authorising Officer's review observations and recommendations.			
Name (Print)		**Position**	
Signature		**Date**	

Principle 1 – Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

1.1 Surveillance camera systems operating in public places must always have a clearly defined purpose or purposes in pursuit of a legitimate aim and be necessary to address a pressing need (or needs). Such a legitimate aim and pressing need include national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. That purpose (or purposes) should be capable of translation into clearly articulated objectives against which the ongoing requirement for operation or use of the systems and any images or other information obtained can be assessed.

1.2 In assessing whether a system will meet its objectives, and in designing the appropriate technological solution to do so, a system operator should always consider the requirements of the end user of the images, particularly where the objective can be characterised as the prevention, detection and investigation of crime and the end user is likely to be the police and the criminal justice system.

1.3 A surveillance camera system should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place. Any proposed extension to the purposes for which a system was established and images and information are collected should be subject to consultation before any decision is taken. When using surveillance systems, you can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent from individuals, or you have a clear obligation or function set out in law.

Principle 2 – The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

2.1 HRA 1998 gave further effect in UK law to the rights set out in the ECHR. Some of these rights are absolute, while others are qualified or limited, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied and the interference is proportionate. The use of surveillance cameras in public spaces places and selected sites could have the potential to impact on human rights including:

- the right to respect for private and family life (Article 8);
- freedom of thought, conscience and religion (Article 9);
- freedom of expression (Article 10);
- freedom of assembly and association (Article 11); and
- protection from discrimination (Article 14).

2.2 The right to respect for private and family life set out in Article 8 of the ECHR enshrines in law a long held freedom enjoyed in England and Wales. People do, however, have varying and subjective expectations of privacy with one of the variables being situational. Deploying surveillance camera systems in public places where there is a particularly high expectation of privacy should only be done to address a particularly serious problem that cannot be addressed by less intrusive means. Such deployment should be subject to regular review, at least annually, to ensure it remains necessary.

2.3 Any proposed deployment that also includes audio recording in a public place is likely to require a strong justification of necessity to establish its proportionality. There is a strong presumption that a surveillance camera system must not be used to record conversations as this is highly intrusive and unlikely to be justified.

2.4 Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose, and be suitably validated. It should always involve human intervention before decisions are taken that affect an individual adversely.

2.5 This principle points to the need for a data protection impact assessment (DPIA) to be undertaken whenever the development or review of a surveillance camera system is being considered to ensure that the purpose of the system is and remains justifiable, there is consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place. Where such an assessment follows a formal and documented process, such processes help to ensure that sound decisions are reached on implementation and on any necessary measures to safeguard against disproportionate interference with privacy.

2.6 A DPIA also helps assure compliance with obligations as data controller under the data protection legislation[footnote 5]. Comprehensive guidance on undertaking a DPIA is available from the ICO. In the case of a public authority, this also demonstrates that both the necessity and extent of any interference with Article 8 and other individual rights has been considered. Relevant authorities should satisfy themselves that a surveillance camera system does not produce unacceptable bias on any relevant ground or characteristic of the individuals whose images might reasonably be expected to be captured by it and operators should take particular account of the Public Sector Equality Duty[footnote 6].

Principle 3 – There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

3.1 People in public places should normally be made aware whenever they are being monitored by a surveillance camera system, who is undertaking the activity and the purpose for which the associated information is to be used. This is an integral part of overt surveillance and is already a legal obligation under DPA 2018. Furthermore, such transparency supports and informs the public and forms part of the wider democratic accountability of surveillance by relevant authorities.

3.2 Responsible and legitimate surveillance is dependent upon transparency and accountability on the part of a system operator. The provision of information is the first step in transparency and is also a key mechanism of accountability. In the development or review of any surveillance camera system, proportionate consultation and engagement with the public and partners (including the police) will be an important part of assessing whether there is a legitimate aim and a pressing need, and whether the system itself is a proportionate response. Such consultation and engagement also provide an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy.

3.3 This means ensuring effective engagement with representatives of those affected and in particular where the measure may have a disproportionate impact on a particular community. It is important that consultation is meaningful and undertaken at a stage when there is a realistic prospect of influencing developments.

3.4 System operators should be proactive in the provision of regularly published information about the purpose, operation and effect of a system. This is consistent with the government’s commitment to greater transparency on the part of public bodies.

3.5 In addition to the proactive publication of information about the stated purpose of a surveillance camera system, good practice includes considering the publication of information on the procedures and safeguards in place, impact assessments undertaken, performance statistics and other management information and any reviews or audits undertaken. Public authorities should consider including this information as part of their publication schemes under the Freedom of Information Act 2000.

3.6 This is not to imply that the exact location of surveillance cameras should always be disclosed if to do so would defeat the justified purpose identified under Principle 1.

3.7 A system operator should have an effective procedure for handling concerns and complaints from individuals and organisations about the use of surveillance camera systems. Information about complaints procedures should be made readily available to the public. Where a complaint is made and the complainant not satisfied with the response, there should be an internal review mechanism in place using a person not involved in handling the initial complaint. Complaints must be handled in a timely fashion and complainants given an indication of how long a complaint may take to handle at the outset.

3.8 Information should be provided to the complainant about any regulatory bodies who may have jurisdiction in that case such as the Information Commissioner or the Investigatory Powers Tribunal.

3.9 Where a complaint or other information comes to the attention of a relevant authority or other system operator that indicates criminal offences may have been committed in relation to a surveillance camera system, then these matters should be referred to the appropriate body, such as the police , the Independent Office for Police Conduct or the ICO for any offences under data protection legislation.

3.10 In line with government commitment towards greater transparency on the part of public authorities, a system operator should publish statistical information about the number and nature of complaints received and how these have been resolved on an annual basis at least.

3.11 The government's further commitment to 'open data' means that public authorities should consider making information available in reusable form so others can develop services based on this data. This would extend to information about surveillance camera systems.

3.12 The Commissioner has no statutory role in relation to the investigation and resolution of complaints. System operators should, however, be prepared to share information about the nature of complaints with the Commissioner on an ad hoc, and where appropriate, anonymised basis to assist in any review of the operation of this code.

Principle 4 – There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

4.1 People considering the need to develop a surveillance camera system should give due consideration to the establishment of proper governance arrangements. There must be clear responsibility and accountability for such a system. It is good practice to have a designated individual responsible for the development and operation of a surveillance camera system, for ensuring there is appropriate consultation and transparency over its purpose, deployment and for reviewing how effectively it meets it purpose.

4.2 Where a system is jointly owned or jointly operated, the governance and accountability arrangements should be agreed between the partners and documented so that each of the partner organisations has clear responsibilities, with clarity over obligations and expectations and procedures for the resolution of any differences between the parties or changes of circumstance. Further guidance on this is available from the ICO.

4.3 A surveillance camera system may be used for more than one legitimate purpose. For example, one purpose might be crime prevention and detection, and another traffic management. Responsibility for each purpose may rest within different elements of a system operator's management structure but overall accountability for ensuring effective governance arrangements and facilitating effective joint working, review and audit, decision making and public engagement sits with the operator.

Principle 5 – Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

5.1 There are significant benefits in having clear policies and procedures for the operation of any surveillance camera system. Where the operator is a relevant authority, their published policies will form part of the body of law under which they operate. Publishing and reviewing their policies and procedures

will aid the effective management and use of a surveillance camera system and ensure that any legal obligations affecting the use of such a system are addressed.

5.2 A surveillance camera system operator is encouraged to follow a quality management system as a major step forward in controlling and improving their key processes. Where this is done through certification against a quality management standard, it can provide a robust operating environment with the additional benefit of reassurance for the public that the system is operated responsibly and effectively, and the likelihood of any breach of individual privacy is greatly reduced.

5.3 It is good practice that the communication of rules, policies and procedures should be done as part of the induction and ongoing professional training and development of all system users. This should maximise the likelihood of compliance by ensuring system users are competent, have relevant skills and training on the operational, technical and privacy considerations and fully understand the policies and procedures. It is a requirement of the data protection legislation that organisations ensure the reliability of staff having access to personal data, including images and information obtained by surveillance camera systems.

5.4 Wherever there are occupational standards available which are relevant to the roles and responsibilities of their system users, a systems operator should consider the benefits and any statutory requirements associated with such occupational standards.

5.5 The Commissioner will provide advice and guidance on relevant quality management and occupational competency standards.

5.6 Wherever a surveillance camera system covers public space, a system operator should be aware of the statutory licensing requirements of the Private Security Industry Act 2001. Under these requirements, the Security Industry Authority (SIA) is charged with licensing individuals working in specific sectors of the private security industry. A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services even where that service is provided by a relevant authority. The SIA can provide more information about licencing requirements.

5.7 SIA licensing is dependent upon evidence that an individual is fit and proper to fulfil the role, and evidence of their ability to fulfil a role effectively and safely with the right skills and knowledge. There are various relevant qualifications available, and training to attain these is delivered by a range of different accredited providers.

5.8 Even where there is no statutory licensing requirement, it is good practice for a system operator to ensure that all staff who either manage or use a surveillance camera system, or use or process the images and information obtained by virtue of such systems have the necessary skills and knowledge.

Principle 6 – No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

6.1 Images and information obtained from a surveillance camera system should not be retained for longer than necessary to fulfil the purpose for which they were obtained in the first place. This is also a requirement of data protection legislation and further guidance on this is available from the ICO.

6.2 The retention period for different surveillance camera systems will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose. It is not, therefore, possible to be prescriptive about maximum or minimum periods. Initial retention periods should be reviewed by a system operator and reset in the light of experience. A proportionate approach should always be used to inform retention periods, and these should not be based upon infrequent exceptional cases.

6.3 Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions, a system operator may need to retain images for a longer period, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Principle 7 – Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

7.1 The sharing of images and other information obtained from a surveillance camera system must be controlled and consistent with the stated purpose for which the system was established. Disclosure of images or information may be appropriate where data protection legislation makes exemptions which allow it, provided that the applicable requirements of the data protection legislation are met, or where permitted by other legislation such as the Counter Terrorism Act 2008. These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime, and for national security purposes. Where a system operator declines a request for disclosure from a law enforcement agency, there is provision under Section 9 of and Schedule 1 to the Police and Criminal Evidence Act 1984 to seek a production order from a magistrate.

7.2 There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. Such requests for images or information should be approached with care and in accordance with the data protection legislation, as a wide disclosure may be an unfair intrusion into the privacy of the individuals concerned.

7.3 A system operator should have clear polices and guidelines in place to deal with any requests that are received. In particular:

- arrangements should be in place to restrict disclosure of images in a way consistent with the purpose for establishing the system
- where images are disclosed, consideration should be given to whether images that may identify individuals need to be obscured to prevent unwarranted identification
- those that may handle requests for disclosure should have clear guidance on the circumstances in which disclosure is appropriate
- the method of disclosing images should be secure to ensure they are only seen by the intended recipient
- appropriate records should be maintained

7.4 Judgements about disclosure should be made by a system operator. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once they have disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image. If the recipient is a relevant authority, it is then the recipient's responsibility to have regard to this code of practice and to comply with any other legal obligations such as data protection legislation and HRA 1998 in relation to any further disclosures.

7.5 Individuals can request images and information about themselves through a subject access request under the relevant part of the data protection legislation. Detailed guidance on this and matters such as when to withhold or obscure images of third parties caught in images is included in guidance issued by the ICO. 7.6 Requests for information from public bodies may be made under the Freedom of Information Act 2000. The ICO also produces detailed guidance on these obligations.

Principle 8 – Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

8.1 Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition systems, or where there is a specific deployment scenario, for example the use of body- worn video recorders.

8.2 Approved standards are available to inform good practice for the operation of surveillance camera systems, including those developed domestically by the British Standards Institute, at a European level by the Comité Européen de Normalisation Électrotechnique or at a global level by the International Electrotechnical Commission.

8.3 A system operator should consider any approved standards which appear relevant to the effective application of technology to meet the purpose of their system and take steps to secure certification against those standards. Such certification is likely to involve assessment by an independent certification body[footnote 7]. This has benefits for a system operator in that the effectiveness of a system is likely to be assured and in demonstrating to the public that suitable standards are in place and being followed.

Principle 9 – Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

9.1 Putting effective security safeguards in place helps ensure the integrity of images and information should they be necessary for use as evidence in legal proceedings. This also helps to foster public confidence in system operators and how they approach the handling of images and information.

9.2 Under the data protection legislation, those operating surveillance camera systems or who use or process images and information obtained by such systems must have a clearly defined policy to control how images and information are stored and who has access to them. The use or processing of images and information should be consistent with the purpose for deployment, and images should only be used for the stated purpose for which collected.

9.3 Security extends to technical and organisational security, including cyber and physical security. There need to be measures in place to ensure appropriate security of the data and guard against unauthorised use, access or disclosure. The ICO publishes helpful guidance on achieving this in practice.

Principle 10 – There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

10.1 A system operator should, as a matter of good governance, review and audit the continued use of a surveillance camera system on a regular basis, at least annually, together with relevant policies to ensure their system remains necessary, proportionate and effective in meeting its stated purpose(s).

10.2 As part of the regular review of the necessity, proportionality and effectiveness of a surveillance camera system, a system operator should assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

10.3 In reviewing the continued use of a surveillance camera system, a system operator should consider undertaking an evaluation to enable comparison with alternative interventions with less risk of invading individual privacy, and different models of operation (to establish for example any requirement for 24 hour monitoring). In doing so, there should be consideration of an assessment of the future resource requirements for meeting running costs, including staffing, maintenance, and repair.

10.4 A system operator should make a summary of such a review available publicly as part of the transparency and accountability for the use and consequences of its operation.

Principle 11 – When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

11.1 The effectiveness of a surveillance camera system will be dependent upon its capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. Wherever the system is used for a law enforcement purpose, it must be capable through processes, procedures and training of system users, of delivering images and information that is of evidential value to the criminal justice system. Otherwise, the end user of the images, who are likely to be the police or a law enforcement agency, will not be able to play their part effectively in meeting the intended purpose of the system – it may be difficult for an operator to argue that their purpose is to detect crime if the quality of the images produced is inadequate to support that purpose.

11.2 It is important that there are effective safeguards in place to ensure the forensic integrity of recorded images and information and its usefulness for the purpose for which it is intended to be used. Recorded material should be stored in a way that maintains the integrity of the image and information, with particular importance attached to ensuring that meta data (e.g. time, date and location) is recorded reliably, and compression of data does not reduce its quality to an extent that it is no longer suitable for its intended purpose. This is to ensure that the rights of individuals recorded by a surveillance camera system are protected and that the material can be used as evidence in court. To do this, the medium on which the images and information are stored will be important, and access must be restricted. A record should be kept as an audit trail of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court. Once there is no longer a clearly justifiable reason to retain the recorded images and information, they should be deleted.

11.3 It is important that digital images and other related information can similarly be shared with ease with appropriate agencies if this is envisaged when establishing a system. If this interoperability cannot be readily achieved, it may undermine the purpose for deploying the system

11.4 It is therefore essential that any digital images and information likely to be shared lawfully with other agencies and the criminal justice system are in a data format that is interoperable and can be readily exported, and then stored and analysed without any loss of forensic integrity. In particular:

- a system user should be able to export images and information from a surveillance camera system when requested
- the export of images and information should be possible without interrupting the operation of the system
- the exported images and information should be in a format which is interoperable and can be readily accessed and replayed

Principle 12 – Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

12.1 Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere, such as databases provided by others, should not be introduced without regular assessment to ensure the underlying data is fit for purpose.

12.2 A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual’s details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.

12.3 When using a surveillance camera system for live facial recognition (LFR) purposes to find people on a watchlist, chief police officers should:

- set out and publish (a) the categories of people to be included on a watchlist and (b) the criteria that will be used in determining when and where to deploy LFR, having regard to the need only to do so for a lawful policing purpose;
- ensure that any biometric data that does not produce an alert against someone on the watchlist by the LFR system is deleted instantaneously or near-instantaneously;
- have regard to the Public Sector Equality Duty, in particular taking account of any potential adverse impact that the LFR algorithm may have on members of protected groups;
- establish an authorisation process for LFR deployments and identify the criteria by which officers are empowered to issue LFR deployment authorisations.

1. Excludes any camera system with relevant type approval of a prescribed device under Section 20 of the Road Traffic Offenders Act 1988 used exclusively for enforcement purposes, which captures and retains an image only when the relevant offence is detected and with no capability to be used for any surveillance purpose. For example, for the enforcement of speeding offences.
2. The Commissioner's functions are set out in Section 34(2) of the 2012 Act: a) Encouraging compliance with the surveillance camera code; b) Reviewing operation of the code, and c) Providing advice about the code.
3. R. (on the application of London Oratory School Governors) v Schools Adjudicator [2015]. See also R (Munjaz) v Mersey Care NHS Trust [2006]
4. Where this is a forensic science activity over which the Forensic Science Regulator has oversight, the Forensic Science Code of Practice applies.
5. Article 35 of the GDPR and Section 64 of DPA 2018.
6. s149 of EA 2010.
7. For instance, the Commissioner's third-party certification scheme. A current list of recommended standards for consideration by a system owner and operator is maintained and made available by the Commissioner. Such a list will provide detailed guidance on suitable standards and the bodies that can accredit performance against such standards

End of document