BECKFOOT TRUST

VIDEO SURVEILLANCE POLICY

V1.1

November 2024

CREATING REMARKABLE SCHOOLS

Table of Contents

1.0 Policy Statement

Beckfoot Trust takes our responsibility towards the safety of pupils, staff and visitors very seriously. To that end, we use CCTV and video surveillance to monitor the members of our local school communities.

2.0 Scope and Purpose

The purpose of this policy is to manage and regulate the use of CCTV and video surveillance at our schools and ensure that:

- we comply with UK General Data Protection Regulations 2018 (UK GDPR) and the Data Protection Act 2018 (DPA 2018)
- the images that are captured are used 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.

This policy covers the use of CCTV, mobile CCTV, drones, and other systems, which capture moving and still images of people who could be identified.

2.1 Video Surveillance Systems

Video surveillance systems within our schools are intended for the purpose of:

- ensuring the welfare of pupils, staff and visitors
- protecting the school buildings and assets, both during and after school hours
- maintaining a safe environment
- deterring criminal acts against persons and property
- assisting the police in identifying persons who have committed an offence
- assisting in student behaviour incidents
- assisting in providing evidence for employee investigations.

This policy relates directly to the location and use of video surveillance systems (including CCTV) and the monitoring, recording and subsequent use of such recorded material. Beckfoot Trust complies with the Information Commissioner's Office (ICO) Guidance on Video Surveillance to ensure it is used responsibly and safeguards both trust and confidence in its use.

The video surveillance systems are included in Beckfoot Trust's registration with the ICO, as a data controller under the terms of the Data Protection Act 2018 and the UK GDPR.

The video surveillance systems are owned and operated by our schools or third-party providers, the deployment of which is determined by the School's Headteacher. **Please note:** *Where the CCTV system is owned and operated by a third party e.g., facilities management or site contractor, a Data Processing Agreement is in place and privacy risks are outlined in a Data Protection Impact Assessment.*

The CCTV systems are closed digital systems which are not recording audio.

Mobile CCTV is a portable system that provides audio and visual recordings of activities undertaken by the wearer and those individuals they interact with.

The video surveillance systems have been designed for maximum effectiveness and efficiency; however, our schools cannot guarantee that every incident will be detected or covered, and 'blind spots' may exist.

The use of drones is prohibited unless express permission has been sought from the Head of Estates for estates related use (e.g., roof surveys) or the Chief Operating Officer for educational or other use, who will ensure that images are limited to the use specified. Great care must be taken not to capture and store images of adjacent properties or the highway. There are specific rules and guidance around the use of drone and the images captured, which need to be taken into consideration.

2.2 Photography and Videoing in a Learning Environment

Please refer to the Trust GDPR Data Protection and FOI Policy.

2.3 Legal Framework

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

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act
- The Freedom of Information Act
- The Human Rights Act
- The Regulation of Investigatory Powers Act
- The Protection of Freedom Act
- The Surveillance Camera Code of Practice issued under the Protection of Freedoms Act
- The Education (Pupil Information) (England) Regulations
- The Local School Standards and Framework Act
- The Children Act
- The Equality Act

This policy will also have regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice' (as amended in 2021)
- Information Commissioner's Office Guidance on Video Surveillance (including guidance for organisations using CCTV)
- Information Commissioner's Office guidance on Drones (www.ico.org.uk)

This policy operates in conjunction with the following Trust policies and procedures:

- Online Safety, ICT and Social Media Policy
- Child Protection and Safeguarding Policy
- UK GDPR, Data Protection and Freedom of Information Policy
- Records Management Procedure
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Procedure
- Data Breach Management Procedure

3.0 Overarching Principles

3.1 Lawfulness, Fairness and Transparency

For any use of video surveillance systems there needs to be a lawful basis for processing personal data under Article 6 of the UK GDPR. Beckfoot Trust processes personal data collected via video surveillance systems under the lawful basis of public task, primarily to ensure the safety and security of pupils, staff and visitors.

Our video surveillance systems do not currently use any biometric data, such as facial recognition technology to uniquely identify individuals.

The cameras making up the fixed CCTV systems are sited so that they only capture images relevant to the purposes for which they have been installed (as described above in section 3), and care has been taken to ensure that reasonable privacy expectations are not violated. The location of equipment is carefully considered to ensure that the images captured comply with the legislation. Every effort will be made to position the cameras so that their coverage is restricted to the school premises, which includes both indoor and outdoor areas.

Mobile CCTV devices will only be used when operationally necessary in support of the purpose outlined above, in section 2.1. Mobile CCTV devices can be switched on or off. If continuous recording is required, strong justification is necessary and therefore it would need to be for a specific purpose, with a Data Protection Impact Assessment in place.

Staff wearing mobile CCTV can switch on the device, when they consider appropriate to do so for the purpose stated in section 2.1. Once the device is switched on, a light on the device will indicate it is recording.

Clear and conspicuous signage have been placed throughout premises where the CCTV surveillance system is active and mobile devices are being used, as mandated by the ICO's video surveillance guidance.

Beckfoot Trust's privacy notices are reviewed periodically or when needed, to ensure information available to data subjects is up to date and accurate.

This policy is available on our Trust's website.

3.2 Specified, Explicit and Legitimate Purpose

Video surveillance systems are used solely for the purposes of ensuring safety and security, preventing and detecting crime, and managing incidents within the school premises.

Further processing for archiving in the public interest, scientific, historical research or statistical purposes shall not be considered to be incompatible with the initial purposes. Schools must record the justification for any such storage of images and discuss with the Risk and Compliance Manager before it takes place.

Any further use of the footage for purposes other than those explicitly stated above, in section 2.1, will not be permitted without the consent of the data subject or unless required by law.

Any member of staff who misuses a surveillance system may be committing a criminal offence and may face disciplinary action.

4.0 Responsibilities and Arrangements

4.1 Data Minimisation

Our schools ensure that video surveillance is targeted and proportionate. Cameras are strategically placed in areas where they are assessed to be needed. They are not used in locations where privacy expectations are unreasonable, such as toilet cubicles or changing rooms.

The extent of surveillance is limited to what is necessary to achieve the intended security objectives.

4.2 Accuracy and Integrity of Data

Our schools take steps to ensure that the video surveillance data collected is adequate, relevant and of sufficient quality to serve its intended purpose.

Regular maintenance checks are performed on the video surveillance systems to ensure they are functioning correctly and capturing clear images.

4.3 Storage Limitation

Video recordings will be retained for a period not exceeding 30 days, in line with the Trust's Data Management Procedure. Once the retention period has expired, the footage will be securely deleted or overwritten to prevent unauthorised access or use.

If the footage is used in an investigation, it will be stored securely and disposed of when the investigation is closed (or as soon as the data has been securely sent/given to a third party such as the police).

4.4 Security

Our schools implement appropriate technical and organisational measures to secure the personal data collected by the video surveillance systems, against unauthorised or unlawful processing, accidental loss, destruction, or damage.

The system will be made secure by the following safeguards:

- The system manager (most senior site manager) will be responsible for overseeing the security of the video surveillance systems, recorded images, maintenance and training of authorised personnel
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible
- Footage will be stored securely and encrypted wherever possible
- Footage will be password protected and any camera operation equipment will be securely locked away when not in use.
- Effective cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

Access to the CCTV and other video systems, software and data will be strictly limited to authorised operators and will be password protected.

Our school's authorised video surveillance system operators must be:

- a limited number of nominated members of staff, approved by the Headteacher.
- the most senior site manager (system manager)

The main control facility is kept secure and locked when not in use. Visual display monitors will be located in secure areas (i.e., a lockable office) and only accessed by authorised persons. The screens must not be easily viewable by unauthorised staff, pupils, or members of the public.

Supervising the access and maintenance of the video surveillance system is the responsibility of the Headteacher. The Headteacher may delegate the administration of the video surveillance system to another staff member. When recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

Live and recorded materials will only be viewed by authorised operators for the purpose of investigating incidents.

At school level detailed records of the processing activities related to video surveillance, including the justification for the use of CCTV, who has access to mobile CCTV devices, locations of cameras, data retention periods, and access logs are maintained.

CCTV systems will be properly maintained at all times, date and time stamps will be checked by the systems manager (the most senior site manager) termly and when the clocks change.

All staff involved in the operation or management of video surveillance systems receive regular training on data protection principles and the lawful use of CCTV and video surveillance.

In the event of a data breach, the school must follow the Trust Breach Management Procedure.

If covert surveillance is being considered, it must be discussed with and approved by the Chief Operating Officer. The Chief Operating Officer will ensure the Home Office's authorisation forms is completed and retained.

4.5 Data Protection by Design and by Default

Beckfoot Trust follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of video surveillance systems, including the replacement, development and upgrading.

Therefore, a Data Protection Impact Assessment (DPIA) will be carried out or reviewed when a system is added, replaced, developed or upgraded to be sure the aim of the system is justifiable, necessary and proportionate.

4.6 Individual Rights and Data Sharing

Under the UK General Data Protection Regulation, individuals have the right to obtain confirmation that their personal information is being processed and have the right to request access to, erasure of or rectification of, their personal data. Please refer to the Trust GDPR, Data Protection and FOI Policy and the Trust Data Subject Access Request Procedure for further information.

There will be no disclosure of personal data to third parties other than authorised personnel such as the Police and other relevant authorities. Requests from the police and other relevant authorities

come in various forms, which will demonstrate the request for information under Schedule 2, Part1 (2) Data Protection Act, the request will need to set out the purpose of the disclosure, information required and needs to be authorised and signed by a police officer of the rank of Inspector or above.

Images may be released to the police for the detection of crime in line with data protection legislation. If an order is granted by a Court for disclosure of video surveillance images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Risk and Compliance Manager should be contacted in the first instance and appropriate legal advice may be required.

Images viewed by the police will be recorded on the Trust's Data Subject Access Request Register and authorised by the school GDPR Lead upon receipt of a valid request. The school GDPR Lead should seek guidance from the Risk and Compliance Manager, if necessary.

5.0 Review of Policy

The Risk and Compliance Manager will review this policy as appropriate and at least on an annual basis.