

CCTV Policy



Approved by: GB

Date: March 2021

Last reviewed on:

Next review due by:

Policy Statement

Introduction

Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the Data Protection Act 2018 and the Information Commissioner's Office (ICO) CCTV Code of Practice. The use of CCTV by schools is covered by the 2018 Act, regardless of the number of cameras or how sophisticated the equipment is.

The School will ensure that the cameras are operated in accordance with the principles in the Human Rights Act 1998.

This CCTV policy explains how The Duston School will operate its CCTV equipment and comply with the current legislation.

Action plan

The school uses CCTV equipment to provide a safer, more secure environment for pupils, staff and visitors and to prevent bullying, vandalism and theft or damage to the school's buildings and/or assets.

Essentially it is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public, pupil and staff safety.
- Monitoring the security of the site.
- To assist in managing the school.

The school does not use the CCTV system for covert monitoring.

Location

Cameras are located in those areas where the school has identified a need and where other solutions are ineffective. The school's CCTV system is used solely for purposes(s) identified above and is not used to routinely monitor staff conduct. Cameras will only be used in exceptional circumstances in areas where the subject has a heightened expectation of privacy. In these areas, the school will use increased signage in order that those under surveillance are fully aware of its use.

Static cameras are not to focus on private homes, gardens and other areas of private property. The planning and design has endeavoured to ensure that the cameras will give maximum effectiveness and efficiency but it is not possible to guarantee that the 3 system will cover or detect every single incident taking place in the areas of coverage.

Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

Maintenance

The CCTV system is maintained by IT services which includes termly checks.

IT services are responsible for:

- Ensuring the school complies with its responsibilities in relation to guidance on the location of the camera.
- Ensuring the date and time reference are accurate.
- Ensuring that suitable maintenance and servicing is undertaken to ensure that clear images are recorded.
- Ensuring that cameras are protected from vandalism in order to ensure that they remain in working order.

Identification

In areas where CCTV is used the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

The signs will:

- Be clearly visible and readable.
- Contain details of the organisation operating the scheme, the purpose for using CCTV and who to contact about the scheme.
- Be an appropriate size depending on context.

Type of equipment

The school's standard CCTV cameras record visual images only and do not record sound. Where two way audio feeds (e.g. call for help systems) are used, they will only be capable of activation by the person requiring help.

Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the School to ensure that the proposed installation is compliant with legislation and ICO guidance.

The School will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

Administration

The school as the data controller has delegated Mr S Strickland - Principal the responsibility for the control of images and deciding how the CCTV system is used. The school has notified the Information Commissioner's Office of both the name of the data controller and the purpose for which the images are used. All operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the CCTV Code of Practice. The day-to-day management will be the responsibility of the Senior Leadership Team, ICT Support and the Site Manager during the day and the Site Team out of hours and at weekends. The CCTV system will be operated 24 hours each day, every day of the year.

Access to recorded images is restricted to staff that need to have access in order to achieve the purpose of using the equipment. All access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images. If the recorded footage reveals that theft has been committed by a member of staff, this evidence may be used in a disciplinary case.

Image storage, viewing and retention

Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. Access to live images is restricted to the CCTV operator unless the monitor displays a scene which is in plain sight from the monitored location.

The viewing of live CCTV images will be restricted to the senior leadership team, the behaviour administrators and IT services.

Recorded images can only be viewed in a restricted area by approved staff [as above]. The recorded images are viewed only when there is suspected criminal activity and not for routine monitoring of pupils, staff or visitors unless the camera(s) are installed to monitor the safe movement of persons through a designated area eg corridors (these areas will be identifiable by clear signs).

No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

The school reserves the right to use images captured on CCTV where there is activity that the school cannot be expected to ignore such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. Images retained for evidential purposes will be retained in a locked area accessible by the system

administrator only. Where images are retained, the system administrator will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed.

Neither the Data Protection Act nor the Information and Records Management Society prescribe any specific minimum or maximum periods which apply to CCTV recorded images. The school ensures that images are not retained for longer than is necessary. CCTV footage is erased automatically after 30 days unless there has been a major incident where footage is downloaded and stored securely in the confidential area of the school server which has restricted access. Once the retention period has expired, these images are removed or erased.

Disclosure

Disclosure of the recorded images to third parties can only be authorised by the Principal who will liaise with the Data Protection Officer.

Disclosure will only be granted:

- If its release is fair to the individuals concerned.
- If there is an overriding legal obligation (e.g. information access rights).
- If it is consistent with the purpose for which the system was established.

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented.

NB: Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

Disclosure may also be made where an order is granted by a Court for disclosure of CCTV images.

Subject access requests

Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the school receives a request under the Data Protection Act it will respond to requests within 1 calendar month of receiving the request. If the school receives a request under the Freedom of Information Act it will respond to requests within 20 school days of receiving the request. As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely as a Freedom of Information request. Those requesting access must provide enough detail to allow the operator to identify that they are the subject of the images, and for the operator to locate the images on the system. Requests for access should be addressed to the data controller.

Refusal to disclose images may be appropriate where its release is:

- Likely to cause substantial and unwarranted damage to that individual.
- To prevent automated decisions from being taken in relation to that individual.
- Likely to involve a disproportionate effort.

Monitoring and evaluation

The school undertakes regular audits to ensure that the use of CCTV continues to be justified. The audit includes a review of:

- Its stated purpose.
- The location.
- The images recorded.
- Storage length.
- Deletion.

Reviewing

The efficacy of this policy will be reviewed annually by the governing body. If the school decides to change the way in which it uses CCTV, it will inform the Information Commissioner within 28 days.

Staff Responsible	TWI		
Date approved by GB:	March 2021	Review Date	March 2022