



CCTV Policy

Reviewed: July 2022

Next Review Due: July 2023

CCTV POLICY

This policy should be read with reference to the Data Protection Act 2018, the Protection of Freedoms Act 2012 and the CCTV code of practice 2008 from the Information Commissioner's Office (ICO) available at:

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

<https://www.legislation.gov.uk/ukpga/2012/9/introduction>

<https://www.enlutc.co.uk/wp-content/uploads/2019/08/cctv-code-of-practice.pdf>

Background

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) has issued a code of practice on compliance with legal obligations under that Act. The use of CCTV by academies is covered by the Act, regardless of the number of cameras or how sophisticated the equipment is and academies should adhere to the ICO's code of practice.

Prior to installation and operation of CCTV, academies should issue a privacy notice to parents/carers and students. They must be clear and transparent in informing students and staff that CCTV will be in operation and about how they will use any personal information they collect. Access to personal information should be restricted only to persons (staff and Trustees) who need particular information to do their jobs, and only when they need it. Where academies wish to use CCTV images in order to make a decision as to whether to conduct a search for an item, this is allowed under the Education Act 2011. However, staff should follow the ICO's CCTV code of practice. Academies can use CCTV in the toilets, but the Data Protection Act 2018 requires that CCTV use maintains privacy.

Objectives and targets

This CCTV policy explains how Plume Academy will operate its CCTV equipment and comply with the current legislation.

Action plan

The academy uses CCTV equipment to provide a safer, more secure environment for students and staff and to prevent bullying, vandalism and theft. 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, student and staff safety.
- Monitoring the security of the site.

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

Location

Cameras are located in those areas where the academy has identified a need and where other solutions are ineffective. The academy'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 e.g. changing rooms or toilets. In these areas, the academy will use increased signage in order that those under surveillance are fully aware of its use.

Maintenance

The CCTV system is maintained by Plume Academy's Site Team and First Ford Ltd under an annual maintenance contract that includes periodic inspections.

The site team/contractors are responsible for:

- Ensuring the academy 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 academy 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 academy'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.

Administration

The data controller (the Premises Manager) has the responsibility for the control of images and deciding in conjunction with the Designated Safeguarding Lead how the CCTV system is used. The academy has notified the Information Commissioner's Office (Reg No: Z3380943) 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. 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 by means of a log book. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images. Under the Schools (Specification and Disposal of Articles) Regulations 2013, academy staff can view CCTV footage in order to make a decision as to whether to search a student for an item. If the recorded footage reveals that theft has been committed by a member of staff, this evidence may also 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. Recorded images can only be viewed in a restricted area by approved staff. The recorded images are viewed only when there is suspected criminal activity and not for routine monitoring of students, staff, or visitors unless the camera(s) are installed to monitor the safe movement of persons through a designated area e.g., corridors (these areas will be identifiable by clear signs).

The academy reserves the right to use images captured on CCTV where there is activity that the academy 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 academy ensures that images are not retained for longer than is necessary. Once the retention period has expired, the images are removed or erased.

Disclosure

Disclosure of the recorded images to third parties can only be authorised by the data controller or DSL.

Disclosure will only be granted if:

- Its release is fair to the individuals concerned.
- There is an overriding legal obligation (e.g., information access rights).
- It is consistent with the purpose for which the system was established.

All requests for access or disclosure are recorded. If access or disclosure is denied, the reason must also be 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.

Data Subject Access Requests (DSAR)

Individuals whose images are recorded have a right to view images of themselves. This right of access is enshrined within Data Protection Law. The appropriate legislation to access CCTV footage of an individual is via a Data Subject Access Request (DSAR). The ICO has guidance about accessing

copies of personal data, including CCTV footage: <https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/>

If the academy receives a request under a Data Subject Access Request, it will comply within 1 calendar month 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 DSAR. 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 or DSL.

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 impede a criminal investigation against any party – unless requested by law enforcement officers.
- Able to show other identifiable people that can be seen in the footage and the Data Manager is unable to edit out those individuals to protect their identity

Monitoring and evaluation

Plume Academy 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 Board of Trustees. If Plume Academy decides to change the way in which it uses CCTV, it will update the office of the Information Commissioner as soon as practicably possible and certainly within 28 days.