

# CCTV POLICY

## 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 1998 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 schools is covered by the Act, regardless of the number of cameras or how sophisticated the equipment is. The Data Protection Act 2018 is also applicable, particularly in relation to any personal data breaches.

## Objectives and targets

This CCTV policy explains how Pippins School will operate its CCTV equipment and comply with the current legislation and the surveillance camera code of practice.

## Action plan

The school already has in place a site security policy. One of its objectives is to ensure that only authorised, proper access to the premises is possible. Appropriately worded signs are displayed indicating opening times of the school and directing visitors to the school office/reception. In addition, appropriately worded warning signs regarding the presence of CCTV are on display.

The Information Commissioner (ICO) is aware that Pippins School operates a CCTV system and that the school uses CCTV equipment to provide a safer, more secure environment for pupils and staff and to prevent bullying, vandalism and theft. Essentially it is used for:

- Monitoring expensive or potentially targeted areas and items (eg IT suite, cycle stores, lockers, science equipment, grounds maintenance equipment) for the prevention, investigation and detection of crime.
- The apprehension and prosecution of trespassers and other offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public, pupil and staff safety (eg monitoring for bullying in communal areas during break times).
- Monitoring the security of the site.
- Supporting the police to deter and detect crime.
- Ensuring that the school rules are respected so that the school can be properly managed.

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 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 (eg changing rooms or toilets). In

these areas, the school will use increased signage in order that those under surveillance are fully aware of its use. The school has ensured that CCTV cameras do not capture images of any properties in the vicinity.

### **Maintenance**

The CCTV system is maintained by Niloc Systems Ltd under an annual maintenance contract that includes periodic inspections.

The contractors are responsible for ensuring that:

- The school complies with its responsibilities in relation to guidance on the location of the camera(s).
- The date and time reference are accurate.
- Suitable maintenance and servicing are undertaken to ensure that clear images are recorded.
- Cameras are protected from vandalism in order to ensure that they remain in working order.
- Any software or other updates to the system are put in place.
- The school's and the contractor's obligations under GDPR are fulfilled.

### **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 (eg call for help systems) are used, they will only be capable of activation by the person requiring help.

### **Administration**

The school's data protection officer is Sapphire Consulting Group Ltd. The data controller for CCTV in the school is the SBM and she reports to the data protection officer. She has responsibility for the control of images and deciding how the CCTV system is 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 ICO's CCTV code of practice and in accordance with GDPR. Access to recorded images is restricted to staff who 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. School staff can view CCTV footage in order to make a decision as to whether to search a pupil for an item. If the recorded footage reveals that theft has been committed by a member of staff, this evidence may be used in a disciplinary case.

If there is a data breach of any kind relating to personal data, then the data processor must notify the data controller without delay and write up a record of the incident. The ICO must be notified within 72 hours. The data controller may have to notify data subjects without undue delay, unless:

- The breach is unlikely to affect their rights.
- The data was adequately protected (eg by encryption).
- Individual notification would be disproportionate.

### **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 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.

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 data controller only. Where images are retained, the data controller will document the reason for its retention, 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. 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. Disclosure will only be granted if:

- Its release is fair to the individuals concerned.
- There is an overriding legal obligation (eg information access rights).
- 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.

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.

### **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 comply with requests within 40 calendar days of receiving the request. The school may charge a fee for the provision of a copy of the images. If the school receives a request under the Freedom of Information Act it will comply with requests within 20 working days of receiving the request. The CCTV system has the facility to mask the identity of any person other than the person requesting access and this facility will be used if the data controller feels it is appropriate. 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.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

Any complaints about the operation of the school's disclosure policy or failure to comply with the ICO code of practice should be addressed through the school's complaints procedure.

### **Monitoring and evaluation**

The school undertakes regular audits to ensure that the use of CCTV continues to be justified and is up-to-date and operates within the ICO code of practice. The policy is evaluated in the light of the findings of the regular audits and any changes in legislation and updated accordingly. The audit includes a review of:

- Its stated purpose.
- The location of cameras.
- The images recorded.
- The secure holding of stored information.
- Storage length of recordings.
- Deletion of recordings.
- Safeguards to protect wireless transmission systems from interception.
- Safeguards to prevent unauthorised copies of information from the CCTV.
- Safeguards where the system is made available across a computer or the intranet.
- Where information is disclosed, how it is securely delivered to the intended recipient.
- Training of staff in security of procedures and sanctions against staff who might misuse surveillance information.
  
- Changes in legislation.

## **Reviewing**

The efficacy of this policy will be reviewed annually by the governing board and in the light of changes to legislation and any concerns brought to their attention about the use of CCTV. If the school decides to change the way in which it uses CCTV, it will inform the Information Commissioner within 28 days.