Applecroft School

CCTV Policy

Person Responsible:	Finance & Business Manager
Review Cycle:	Annually
Reviewed Date:	May 2026
Next Review Date:	May 2027

CCTV Policy

School Vision:
'To be a positive and inspiring community that nurtures each individual and empowers leaders for life'.

School Mission Statement:
'Nurturing Potential, Inspiring Minds, Changing Lives'

School Values:

- Ambition and Leadership
- Kindness and Supportiveness
- Respect and Honesty
- Determination and Resilience

Policy statement and objectives

Applecroft School has in place a CCTV surveillance system on its site. The purpose of this policy is to set out the responsibilities of the school regarding the management, operation and use of the CCTV system, and details the procedures to be followed in order to ensure that the school complies with relevant legislation.

This policy applies to all members of our staff, visitors to the site and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance, including:

- UK General Data Protection Regulation ("UK GDPR")
- Data Protection Act 2018
- CCTV Code of Practice produced by the Information Commissioner's Office (ICO)
- Human Rights Act 1998
- Freedom of Information Act 2000

Introduction

The information held by organisations that is about individuals is covered by the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) and the guidance in this policy will help Applecroft School comply with their legal obligations.

The DPA 2018 and UK GDPR not only create obligations for organisations, they also give individuals rights, such as the right to access their personal information, and to claim compensation when they suffer damage.

When using, or intending to use surveillance systems, many organisations also need to consider their obligations in relation to the Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act (POFA), the Human Rights Act 1998 (HRA) and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA code).

The DPA 2018 and UK GDPR are applicable to all organisations that process personal data across the whole of the UK and has the same effect across all sectors. One of the key differences is that the private sector is required to follow the data protection code of practice to meet its legal obligations under the DPA 2018. Any organisation using cameras to process personal data should follow the recommendations of this code.

About the Data Protection Code of Practice

Each section of the code poses questions that must be addressed to help ensure that good practice recommendations are achieved.

Following the recommendations in this code will:

- help ensure that those capturing individuals' information comply with the DPA 2018, UK GDPR and other relevant statutory obligations;
- contribute to the efficient deployment and operation of a camera system;
- mean that the information captured is usable and can meet its objectives in practice;

- reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- re-assure those whose information is being captured;
- help inspire wider public trust and confidence in the use of CCTV; and
- help organisations in England and Wales to follow guidance in the POFA code.

The majority of surveillance systems are used to monitor or record the activities of individuals, or both. As such they process individuals' information - their personal data. Most uses of surveillance systems will therefore be covered by the DPA 2018, UK GDPR, the provisions of the Data Protection code of Practice and this policy.

Purpose of the CCTV system

The principal purposes of the CCTV system are as follows:

- to ensure the safety of staff, students and visitors;
- for the prevention, reduction, detection and investigation of crime and other incidents;

The school intends to use CCTV for the purposes of:

- providing a safe and secure environment for pupils/students, staff and visitors;
- protecting the school buildings and assets, both during and after hours;
- assisting in the prevention of crime and assisting law enforcement agencies in apprehending offenders

The use of the CCTV system will be conducted in a professional, ethical and legal manner and only for the intended purposes.

Governance

Ensuring effective administration

Establishing a clear basis for the processing of any personal information is essential, and the handling of information relating to individuals collected from surveillance systems is no different. It is important that you establish who has responsibility for the control of this information, for example, deciding what is to be recorded, how the information should be used and to whom it may be disclosed.

As Applecroft School makes the above decisions they are acting as the data controller and are legally responsible for compliance with the DPA 2018 and UK GDPR and must also notify the ICO that they are acting as the data controller.

Ensuring clear procedures to determine how you use the system in practice.

- The CCTV system is used for the purpose of crime prevention and is positioned in various easily identifiable positions around the exterior of the school/car park. Those who have responsibility for operating the system are aware of its specific purposes.

- The CCTV system operates to meet the requirements of the current data protection legislation and the ICO's guidance.

- There are clearly documented procedures within the school's Data Protection Policy, based on the Data Protection Code of Practice, for how information will be handled in practice. These include guidance on disclosures and how to keep a record of these. All staff have received training on the school's Data Protection Policy and a copy is available on the school's website.

- The responsibility for ensuring that procedures are followed has been allocated to the school's Business Manager. The Business Manager ensures that standards are set, procedures are put in place to meet these standards, and that the system complies with the Data Protection Code of Practice and legal obligations, such as an individual's right of access.

- Proactive checks are carried out on a regular basis to ensure that procedures are being complied with. This is done by the school's Business Manager

- The use of surveillance systems is regularly reviewed to ensure it comprises use continues to be justified.
- The system currently comprises fixed external cameras. The school has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.
- Cameras are sited to ensure that they only capture images relevant to the purposes for which they are installed.
- Cameras are placed so as to record external areas in such a way as to prevent or minimise recording of passers-by or of another person's private property. Care has been taken to ensure that reasonable privacy expectations are not violated.
- CCTV warning signs are clearly and prominently placed at all external entrances to the site. Adequate signage is placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Signs contain details of the purpose for using CCTV.
- Annually, the school renews its notification with the ICO.

Looking after the recorded material and using the information

Storing, monitoring and recording surveillance system information

Recorded material is 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 effectively for its intended purpose. To do this the school has carefully chosen how the information is held and recorded, and ensures that access is restricted. The school also ensures that the information is secure and where necessary, encrypted. Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system.

In the event that surveillance information will be needed as evidence in court the school keeps a record or audit trail showing how the information is handled. Once there is no reason to retain the recorded information, it is deleted. A record or audit trail of the deletion process is also captured.

Monitoring and Recording

The viewing of live CCTV images and recorded images which are stored by the CCTV system is restricted to authorised staff with the required security access. The CCTV monitor is situated in the Site Manager's Office. Access to view CCTV images is restricted to personnel who have legitimate access to the Site Manager's Office and further restricted to those members of staff with authorisation to access the CCTV system.

All authorised operators and staff with access to images are aware of the procedures that need to be followed when accessing the recorded images. All staff are aware of the restrictions in relation to access to, and disclosure of, recorded images.

Relevant images may be shared with Board of Trustees panels reviewing exclusions, disciplinary matters or complaints.

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 the disclosure of images.

Monitoring and recording of Public Areas may include the following:

- the building's perimeter, main entrance/exit gates, lobbies and corridors, storage areas;
- restricted access areas at entrances to buildings and other areas;
- door controls, external alarms;
- parking areas, adjacent public highway

Storage of Images

The images/recordings are stored in a secure environment with a log of access kept.

Access is restricted to authorised personnel only.

Disclosure

Disclosure of information from surveillance systems is controlled and consistent with the purpose(s) for which the system was established. For example, it can be appropriate to disclose surveillance information to a law enforcement agency when the purpose of the system is to prevent and detect crime, but it would not be appropriate to place them on the internet in most situations.

Arrangements are in place to restrict the disclosure of information in a manner that is consistent with the purpose for establishing the system.

- The person designated to handle requests for disclosure has clear guidance on the circumstances in which it is appropriate to make a disclosure and when it is not.
- The school records the date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) and why they required it.
- When disclosing surveillance images of individuals, particularly when responding to subject access requests, the person designated to handle requests considers whether the identifying features of any of the other individuals in the image need to be obscured.
- Once you have disclosed information to another body, such as the police, they become the data controller for the copy they hold. It is their responsibility to comply with the DPA 2018 and UK GDPR in relation to any further disclosures.

Subject access requests

Individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information.

Providing information promptly is important, particularly where you may have a set retention period which will mean that the information will have been routinely deleted

In such circumstances, as good practice, the school will put a hold on the deletion of the information.

Those who request access must provide you with details that allow you to identify them as the subject of the information and also to locate the information on your system. The school considers:

- how staff involved in operating the surveillance system will recognise a subject access request; and
- whether internal procedures for handling subject access requests are in place. This includes keeping a log of the requests received and how they were dealt with, in case the school is challenged.

The school's surveillance system allows it to easily locate and extract personal data in response to subject access requests. It is designed to allow for the redaction of third party data where this is deemed necessary.

Where a subject access request is received for surveillance footage or other information, the school will provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. This is done by supplying them with a copy of the information in a permanent form.

Freedom of information

Being a public authority the school may receive requests under the FOIA. The school has a member of staff who is responsible for responding to freedom of information requests, and understands their responsibilities. They will respond within 20 working days from receipt of the request.

If a request for surveillance system information is received, the school would consider:

- Is the information personal data of the requester? If so, then that information is exempt from the FOIA and FOISA. Instead, this request is 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.

Retention

The DPA 2018 and UK GDPR do not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Rather, retention should reflect the organisation's purposes for recording information. The retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. It should not be kept for longer than is necessary, and should be the shortest period necessary to serve the school's purpose.

The school will not keep information for longer than strictly necessary to meet the purposes for recording it. On occasion, the school may need to retain information for a longer period, where a law enforcement body is investigating a crime and asks for it to be preserved, to give them opportunity to view the information as part of an active investigation.

The school has decided on the shortest period that they need to retain information, based upon their purpose for recording it.

- The school's information retention policy documents that the school's CCTV data retention period is set at 30 days.

- Measures are in place to ensure the permanent deletion of information through secure methods at the end of the 30 day period.

- The school undertakes systematic checks to ensure that the retention period is being complied with.

Staying in control

It is essential that the school ensures that it continues to comply with the DPA 2018, the UK GDPR and the requirements of the Data Protection Code of Practice. To comply with this the school:

- tells people how they can make a subject access request, who it should be sent to and what information needs to be supplied with their request;
- gives them a copy of this policy or details of the ICO website; and
- tells them how to complain about either the operation of the system or failure to comply with the requirements of this policy.

Staff using the surveillance system or information from the surveillance system are trained to ensure they comply with this policy. In particular, they know:

- What the organisation's policies are for recording and retaining information.
- How to handle the information securely.
- What to do if they receive a request for information, for example, from the police.
- How to recognise a subject access request and what to do if they receive one.

All information is sufficiently protected to ensure that it does not fall into the wrong hands. This includes technical, organisational and physical security. Applecroft ensures that:

- There are sufficient safeguards in place to protect wireless transmission systems from interception.
- The ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place for when the system is connected to, or made available across, a computer, e.g. an intranet.
- Where information is disclosed, that it is safely delivered to the intended recipient.
- Control rooms and rooms where information is stored are secure.

- Staff are trained in security procedures and there are sanctions against staff who misuse surveillance system information.

Complaints Procedures

Complaints concerning the school's use of its CCTV system or the disclosure of CCTV images should be made in writing to the school's DPO, Mrs Odette Coe, Finance & Business Manager, admin@applecroft.herts.sch.uk

Selecting and siting surveillance systems

The information collected by a surveillance system must be adequate for the purpose you are collecting it. The type of surveillance system you choose and the location it operates within must also achieve the purposes for which you are using it. You should ensure that the design of any surveillance systems you purchase allows you to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third party data where this is deemed necessary.

Both permanent and movable cameras should be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property. The cameras must be sited and the system must have the necessary technical specification to ensure that unnecessary images are not viewed or recorded, and those that are recorded are of the appropriate quality.

As data controller, the school is responsible for ensuring that the design of any surveillance systems purchased allows you to easily locate and extract personal data in response to subject access requests. They should also be designed to allow for the redaction of third party data where this is deemed necessary.

Surveillance systems should not normally be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified.

Prior to the installation or repositioning of any CCTV camera, or system, a data protection impact assessment (DPIA) is required to be conducted by the school to ensure that the proposed installation is compliant with legislation and ICO guidance. The assessment is approved by the DPO.

The school has adopted 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.

Letting people know

You must let people know when they are in an area where a surveillance system is in operation.
The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area.

Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Signs should:

- be clearly visible and readable;
- contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact about the scheme (where these things are not obvious to those being monitored);
- include basic contact details such as a simple website address, telephone number or email contact

Signs on roads

Appropriate signs must be provided to alert drivers to the use of cameras on the road network or in areas that vehicles have access to, such as car parks.

Signs must make clear that cameras are in use and explain who is operating them, so that individuals know who holds information about them and therefore have the opportunity to make further enquiries about what is happening with their data.

Appendix 1 – information for signs

This CCTV system and the images produced by it are controlled by the Finance & Business Manager who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose which is a legal requirement of the Data Protection Act 2018.
Applecroft School have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of all those who use school. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Appendix 2 – Checklist for users of CCTV systems

	Checked Date	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			

There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			

Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			