HOOK INFANT SCHOOL

CCTV SYSTEM POLICY

INTRODUCTION

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television system (CCTV) at Hook Infant School, hereafter referred to as 'the School'.

The system comprises a number of fixed and dome cameras located around the School site. All cameras are monitored from a central location and are only available to selected staff.

The Policy and Code of Practice will be subject to regular review.

The CCTV systems listed in the school's Site-Specific Code of Conduct are wholly owned by the School.

OBJECTIVES OF THE CCTV SYSTEM

a) To protect the School buildings and their assets
b) To increase personal safety and reduce the fear of crime
c) To support the Police in a bid to deter and detect crime
d) To assist in identifying, apprehending and prosecuting offenders
e) To assist in managing the School

THE REGULATORY LANDSCAPE

UK GDPR/DATA PROTECTION ACT 1998 (DPA)

The UK GDPR/DPA applies to all operators of CCTV where the use of the system involves the processing of personal data which will include footage from CCTV cameras of individuals or information that relates to them from which they can be identified.

THE ICO'S CCTV CODE OF PRACTICE – KEY REQUIREMENTS

Assess the risk - in particular, before installing CCTV, the code expects organisations to first consider the impact of their proposed use of CCTV on people's privacy.

Internal controls and procedures - the code goes on to give guidance on the checks and balances needed around the handling of images, including whether the organisation responsible for the system has notified the ICO that they are a data controller, the purpose of the processing of images as well as how and under what circumstances these may be disclosed, among other details.

Other checks should include procedures for how the images will be handled and ensuring that the responsibility for delivering compliance with these procedures within the organisation is allocated to a named individual.

Selecting and siting cameras - guidance is provided in the code on selecting and siting cameras to make sure these only record what is relevant at a time when this is relevant and that any captured images are of the right quality. The code warns against siting cameras in places where people would have a higher expectation of privacy such as changing rooms or toilets.

Use of CCTV Equipment - the code recommends in addition to ensuring good image quality, that other features of the system are appropriate and fit for purpose such as:

- ensuring any date and time stamps recorded to images are correct;
- ensuring where wireless transmission of digital image data is involved, that adequate measures have been taken to secure the data stream from unauthorised interception.

Audio recording of conversations by CCTV should not typically be enabled unless exceptional circumstances apply such as with audio help points covered by CCTV activated by a member of the public or the use of specific recording (and only)where it is made very clear that audio recording may also occur.

Look after recordings - operators of CCTV are expected to make sure that recordings are stored in such a way that image quality is preserved and images can easily be extracted from systems when required by law enforcement agencies. The images must remain secure and only be viewed under restricted conditions with access limited only to authorised personnel.

Image storage should be for no longer than is required for the organisation's own purpose, and only held beyond this if needed by law enforcement agencies investigating a crime. When no longer required then image deletion must be thorough and secure.

Generally speaking, disclosures should be limited to circumstances such as preventing or detecting crime or where people ask to view images of themselves provided that in both cases, the disclosures are subject to clearly documented processes, including considering if providing images may unfairly intrude on the privacy of any third party and, if so, making sure these images are obscured.

Publicising the use of CCTV - importantly, operators of CCTV are expected by the code to make clear to people when they are entering and are within an area under CCTV surveillance through signs that are:

- clear, prominent, readable;
- identify the operator of the system, giving details of who to contact about its use; and explain the purpose of the CCTV.

Separate, specific guidance on the use of CCTV in the workplace is also provided in the ICO's Employment practices Code.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)/INVESTIGATORY POWERS ACT 2016/18

Part II of RIPA regulates covert surveillance by public authorities using, among other things, CCTV. Following concerns that public authorities were using powers under RIPA to conduct surveillance that was out of proportion to the minor nature of the offences under investigation, RIPA was amended by Part 2 of the Protection of Freedoms Act in November 2012 (see below) to require designated public authorities to obtain the prior approval of a magistrate for any covert surveillance authorised under RIPA.

FREEDOM OF INFORMATION ACT 2000 (FOIA)

Where public authorities operate CCTV then they may receive requests under the FOIA for recorded information held by them or on their behalf. Requests received under the FOIA must be responded to within 20 working days of receiving the request.

Where the requested footage contains images about individuals then an exemption under s40 of the FOIA covering personal data of individuals may be relevant. In particular, where the requested images are those of the requestor, then the information is exempt under the FOIA and the request should instead be treated as a request made under the separate subject access provisions of the DPA (see above). However, where images include other people, then whether it is possible to release this information under the FOIA will depend on whether disclosure would breach the data protection principles and, in particular, whether under the first principle, the processing would be unfair to the subjects of the footage.

PROTECTION OF FREEDOMS ACT 2012

In line with a public intention of the coalition government to limit state surveillance, A Surveillance Camera Code of Practice (SCCP) was published in July 2013, under the Protection of Freedoms Act 2012.The code applies to the appropriate and effective use of CCTV systems in public places by 'relevant authorities' such as local authorities and policing authorities, regardless of whether or not there is any live viewing or recording of images, information or data. Others who use CCTV are also encouraged to abide by its terms. Covert surveillance is not covered by the code but is instead subject to the separate RIPA and DPA (see above).

The SCCP sets out twelve principles that CCTV system operators should adopt and designate responsibility for ensuring compliance with the code.

SCCP Guiding Principles

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet a pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted when their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

STATEMENT OF INTENT

The CCTV Scheme is registered with the Information Commissioner under the terms of the GDPR/DPA and will seek to comply with the requirements both of the legislation and the Information Commissioner's Code of Practice.

The School will treat the system and all information, documents and recordings obtained and used as data which are protected by the GDPR/DPA.

Cameras will be used to monitor activities within the school grounds to identify criminal activity actually occurring, anticipated or perceived and for the purpose of securing the safety and well being of the School, together with its visitors.

Cameras will not focus on private homes, gardens and other areas of private property.

Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the School's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Information will only be released to the Media for use in the investigation of a specific crime and with the written authority of the Police. Information will never be released to the Media for purposes of entertainment.

The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the School CCTV.

Note:

- Parents and children of Hook Junior School who use the path through our site, from our main car park to their school gate, will be recorded by our cameras while on the school premises.
- Our system partially covers the joint courtyard area between the two schools to monitor access to this area from the Infant School. As a result part of the Junior School's section of the courtyard is also monitored by our CCTV system and Junior School staff and pupils will be recorded while in the area covered by our camera.
- Infant School staff and pupils will be recorded by the Junior School CCTV system from one of their cameras at the rear of the Year 2 building and Sensory Garden.

Operation of the System

The scheme will be administered and managed by selected staff in accordance with the principles and objectives expressed in the code: - Headteacher, Deputy Headteacher and Network Manager/DPO. This policy and the school's Site Specific Code of Practice will be followed at all times. The CCTV system will be in operation continuously.

Other administrative functions will include maintaining the hard disc space, filing and maintaining occurrence and system maintenance logs. Emergency procedures will be used in appropriate cases to call the Emergency Services. Liaison meetings may be held with all bodies involved in the support of the system.

Monitoring Procedures

Camera surveillance may be maintained at all times.

In order to maintain and preserve the integrity of the recordings from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to.

a) Recordings required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate secure place. If a recorded image is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by a controller, dated and returned to the evidence store.

b) If an image is archived the reference must be noted.

c) Recordings may be viewed by the Police for the prevention and detection of crime, authorised officers of Hampshire County Council for supervisory purposes, authorised demonstration and training.

d) A record will be maintained of the release of images to the Police or other authorised applicants. A register will be available for this purpose.

e) Viewing of images by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

f) Should an image be required as evidence, a copy may be released to the Police under the procedures described in paragraph 5 (a) of this code. Images will only be released to the Police on the clear understanding that the recording/image remains the property of the School and both the recording/image and information contained on it are to be treated in accordance with this code. The School also retains the right to refuse permission for the Police to pass on to any other person the recording/image or any part of the information contained therein. On occasions when a Court requires the release of original data, this will be produced from the secure evidence store complete in its sealed bag.

g) The Police may require the School to retain the stored data for possible use as evidence in the future. Such information will be properly indexed and properly and securely stored until they are needed by the Police.

h) Applications received from outside bodies (e.g Solicitors) to view or release recordings/images will be referred to the Head Teacher. In these circumstances information will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request or in response to a Court Order. See the Data Protection Policy, Subject Access Request Procedure and Privacy Notices for more information.

Breaches of the code

Any breach of the Code of Practice by School Staff will be initially investigated by the Head Teacher, in order for her to take the appropriate disciplinary action. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

Assessment of the scheme and Code of Practice

Performance monitoring, including random operating checks may be carried out.

Public Information

Copies of this Policy and the Code of Practice will be available to the public from the School Office and the school's website.

Complaints

Any complaints about the Schools CCTV system should be addressed to the Head Teacher. Complaints will be investigated in accordance with section 6 of this code.

Access by the Data Subject

The UK General Data Protection Regulation and the Data Protection Act 2018 provide Data Subjects (individuals to whom 'personal data' relate) with a right to data held about themselves, including those obtained by CCTV. To make a request for your personal information, or be given access to your child's educational record, contact our Headteacher, Business Manager or Data Protection Officer at the school office.

Data subjects also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

For more information on making a Subject Access Request please read our "Subject Access Request Procedure"

Contact
If you would like to discuss anything in this policy, please contact the school's Data Protection Officer as listed below.

Data Protection Officer	Peter West Hook Infant School, Church View, Hook, Hampshire. RG27 9NR
Telephone:	01256 764489
Email:	dpo@hook-inf.hants.sch.uk

Approved by the Governing Body, Hook Infant School

Reviewed and revised: November 2021

Signed *Alison Collier*

Chairman of Governing Body

Date: 17 November 2021

Date for Review: November 2024