HILDERTHORPE PRIMARY SCHOOL

CCTV Policy and Code of Practice

Effective Date:	**23/04/2024**
Amended:	
Date Due For Review	**22/04/2025**
Contact Officer:	**School Business Manager**
Approved By:	**Governing Body**

1. Background

Surveillance cameras are used by Hilderthorpe Primary School in a number of areas and are a valuable tool to assist in areas such as public and employee safety, enhancing security and in protecting property.

The camera installations are owned by Hilderthorpe Primary School and are operated in line with data protection legislation, the Human Rights Act 1998 and guidelines, such as those issued by the Information Commissioner's Office (ICO) and the Surveillance Camera Commissioner, to ensure, for example, that the need for public protection is balanced with respect for the privacy of individuals.

2. Definitions for the Purposes of this Code

For the purposes of this policy, the following definitions apply in relation to Data Protection.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

System Manager – the person with day to day responsibility for making decisions about how the cameras are used and the processing of images captured, including maintaining the relevant code of practice.

Overt surveillance - means any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act (RIPA) 2000.

Covert surveillance - is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place.

Surveillance camera systems - is taken to include: (a) closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c).

3. Policy Statement

This policy applies to all overt surveillance cameras controlled by Hilderthorpe Primary School as a data controller.

Surveillance cameras are a valuable resource, which help the school in areas such as protecting the public and its employees, enhancing security, crime prevention and protecting property. Hilderthorpe Primary School recognises that whilst there is a high level of public support for surveillance camera schemes, there are also increasing concerns about the role of cameras and their impact upon the privacy of members of the public, employees, parents and students.

To help address these concerns Hilderthorpe Primary School is committed to ensuring compliance with data protection legislation, the Human Rights Act 1998 and all relevant guidelines issued by the ICO and Surveillance Camera Commissioner. Hilderthorpe Primary School regards the lawful use and correct installation of surveillance cameras as

essential to its successful operations and to maintaining confidence between the School and those with whom it carries out business. The School fully endorses the twelve guiding principles set out in the Surveillance Camera Code of Practice (see section 7) and is committed to privacy by design and default.

4. Identified Key Risk Factors

Hilderthorpe Primary School as data controller have identified the following risk factors.

Fraud / Theft / Wilful Damage / Breaches of Security / Use of Violence / Instances of Crime

5. Purpose of the System

- Prevent, investigate and detect crime
- Help reduce the fear of crime
- Assist with the apprehension and prosecution of offenders
- Enhance the safety of employees and the public
- To safeguard vulnerable adults and children
- Provide evidential material for court or committee proceedings
- Reduce incidents of public disorder and anti-social behaviour
- Evidence in investigations of gross misconduct (including protecting employees from allegations)
- Protect property
- Process Subject Access Requests

6. Camera Locations and Associated Coverage Linked to Perceived Risk Factors

Ref	Location	Line of Site	Fixing	Risk indicator

1	Pole at Front Entrance to School pointing towards gates.	Main Entrance	Static	Theft / Damage / Violence / Breaches of Security
2	Outside reception pointing towards EYFS outside area	Reception and EYFS outside area	Static	Theft / Damage / Violence / Breaches of Security
3	Above the boiler room door pointing towards the MUGA	Playground and MUGA	Static	Theft / Damage / Violence / Breaches of Security
4	Above the kitchen window	Playground and trim trail	Static	Theft / Damage / Violence / Breaches of Security

7. Guiding Principles

Hilderthorpe Primary School will follow 12 guiding principles set out in the Surveillance Camera Code of Practice when operating surveillance cameras:

1. 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 an identified pressing need.

2. 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.

3. 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.

4. There must be clear responsibility and accountability for all surveillance camera system activities, including images and information collected, held and used.

5. 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.

6. 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 once their purposes have been discharged.

7. 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.

8. 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.

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

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement, with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

Data protection legislation also requires the School to comply with the six data protection principles if it is processing personal data.

8. Control of Access to System and Images

The viewing of live time imagery captured on overt cameras that duplicate what is in general public view is acceptable. However, caution and discretion is advised at all times. Where possible, display screens should be placed in locations away from public view.

Cameras are monitored through a terminal which is located in the locked Server Room and the recording equipment also located in the locked Server Room.

Screens should be switched off at all times unless the camera is to be used for the purpose for which it was designed; this will avoid 'unintentional' viewing of unrelated imagery.

The Head Teacher and the School Business Manager will be the system managers and will hold the administrator's password and the right to allocate passwords to users of the system.

The named persons with associated levels of access rights to surveillance system are:

Ref	Staff Name, Job Role	Access Level
1	School Link DPO - School Business Manager	Full Access
2	Head Teacher – Mrs S Hall	Full Access
3	Deputy Head - Mrs J Grant	Full Access

All authorised users of the system must be trained in the use of the system and must have read the Code of Practice and procedures in relation to its use. Once training is complete, each authorised user will sign a training register to verify that they understand how to use the system. The training register is kept In the Server Room with the System Log Book.

9. Camera System Checks and Maintenance

A monthly assessment of the system will be carried out by the school caretaker to ensure that all cameras are receiving an image (basic functionality) and that the time and date shown on the images are correct. All instances of camera malfunction must be reported as soon as possible, to the current maintenance contractor engaged for annual inspection and for repairs.

Image capture quality must also be tested on a monthly basis. The functioning camera is to be selected and the images produced tested for clarity (in case of the need for production of images for use, in cases of criminal prosecution).

Records of the tests are to be recorded in the system log book located in the locked Server Room.

10. Retention of Recorded Images

Images recorded onto the hard drive of the CCTV systems shall be retained for a period of less than 14 days (unless images are being used for an ongoing investigation).

At the end of the 14 day period, images are overwritten automatically (by earliest date of recording first) or can be saved by an authorised named person if an investigation is ongoing.

This action must be recorded in the system log book, detailing date period, by whom and why the images are being retained.

Any images that may have been saved must be deleted after a period of 3-6 calendar months of retention, unless a specific request has been received stating otherwise.

11. Reference Tables in Use

Not in use

12. Disclosure of Images

Any request by an outside organisation or individual (SAR), for access to recorded or real time CCTV images must be passed to the schools Data Protection Officer for logging and authorisation.

Should the request be a 'simple', unobtrusive request, this may be dealt with on site by the School Business Manager.

Imagery must be reviewed by the authorised named person, taking into account any possible third party inclusion in images. Every effort should be made to protect third party privacy.

Should the authorised named person feel that any third party would not have their basic right to privacy infringed, they may offer the individual/organisation requesting sight of the imagery, the opportunity to 'view' the recorded data.

Should the individual then go on to request a copy of the imagery, this must be referred to the school's Data Protection Officer for authorisation. The appropriate request form must be completed and a record made within the system log book.

Should the school receive a request for CCTV footage from the Police the following Police requests do not require prior authorisation. However the member of staff dealing with the request must be confident that there is a need to share the information and a log must be kept:

- Police requests relating to an immediate danger to the public/staff.
- Requests which relate to crimes the school has reported to the Police.

Once completed, details must be logged as with any other request.

If the request cannot be dealt with immediately, copied images must be held securely on the Headteachers Computer as outlined in section 6.

13. Signage

Appropriate signage shall be displayed in the following : Front Entrance to the School

14. References

Human Rights Act 1998
Data Protection Act 2018
General Data Protection Regulation
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000

Protection of Freedoms Act 2012

ICO CCTV Code of Practice - https://ico.org.uk/code-of-practice