CCTV Policy

Prepared By:	Director of IT		
Approved By:	DCEO	Date:	September 2024
Start Date:	September 2024	Review Date:	September 2025

1. Introduction

This Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) at Harefield Primary School. A Data Protection Impact Assessment (DPIA) has been [will be] carried out prior to the first use of the CCTV system. If there are changes to the CCTV system further DPIA will be carried out.

2. Purpose and Objectives of the CCTV Scheme

- To increase personal safety of students, staff and visitors and reduce the fear of crime
- To promote the health and safety of staff, pupils and visitors as well as for monitoring pupil behaviour
- To assist in managing the school
- To protect the school buildings and their assets
- To monitor and minimize unauthorized and inappropriate vehicle access
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property

The school's legal basis under Article 6 GDPR for our use of CCTV is that the processing is necessary for the school to perform a task in the public interest or for the school's official functions.

3. Statement of Intent

- The school has regard to the Information Commissioner's Office (ICO) CCTV code of practice www.ico.org.uk to ensure CCTV is used responsibly and safeguards both trust and confidence in its use. The school also has regard to the Surveillance Camera Code of Practice https://www.gov.uk/government/publications/surveillance-camera-code-of-practice and adopts the 12 guiding principles in the code which are set out the appendix to this policy.
- For the purposes of registration under the Data Protection Act 2018 and GDPR, the school is registered under the Hamwic Education Trust (Data Controller), registration number ZA265013.
- The school will treat the system, and all information, documents and recordings obtained and used as data.
- Cameras will be used to monitor activities within the school and grounds in line with the objectives of the scheme.
- Static cameras are set as to not focus on private homes, gardens and other areas of private property.
- Materials, or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purposes. Recordings will only be released under written authority from the Police, or in respect of a subject access request (please see the Data Protection Policy).
- 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.

4. CCTV Systems

- The system comprises of fixed cameras around the school site
- The system does not have sound recording enabled
- The system is owned and operated by the school
- Access to the system is determined by the School Senior Leadership Team

5. CCTV System Operation

- The School Leader is responsible for the operation of the CCTV system and for ensuring compliance with this policy.
- Access to the system will only be granted by the School Leader, in a clear written communication to the member of staff being granted access, stating the reason for the access and under what circumstances the member of staff is authorized to use the system.
- Access to the CCTV system and recorded data will be strictly limited to authorized members of staff.
- Breaches of the policy by staff using and/or monitoring the system for non-work related matters, i.e. for their own recreation or interest may constitute matters of discipline under the relevant conditions of their employment.

  Users should;

  - Be provided with a unique password
  - Be shown how to use the system
  - Read and confirm in writing that they have understood the CCTV policy

- The CCTV system will be operated 24 hours each day, every day of the year.
- Those with authorized access must be aware of who is around them when viewing images.
- The system will be checked by the site manager, on a weekly basis to ensure that it is running effectively, and that the system is recording properly and the cameras are operating.

6. CCTV Location

- The cameras are sited so that they only capture images relevant to the purposes for which they are installed, and care is taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation.
- The school makes every effort to position cameras so that their coverage is restricted to the school premises, which may include both indoor and outdoor areas.
- CCTV will not be used in standard classrooms, however, may be positioned in areas of high value such as ICT suites, as well as in areas of higher risk for student and staff protection or areas within the school that have been identified as not being easily monitored.
- The school will keep an updated location map of the CCTV cameras.
- Staff will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

7. Signage and Privacy Notices

- It is a requirement of the Data Protection Act 2018, to notify people entering a CCTV protected area to inform that that the area is monitored by CCTV and that pictures are recorded. The CCTV sign should include the following:
    - That the area is covered by CCTV surveillance and pictures are recorded
    - The purpose of using CCTV
    - The name of the school
    - The contact telephone number and/or address for enquiries
- Warning signs are placed at all access routes to areas covered by the school's CCTV.
- The school's use of CCTV is covered by a privacy notice which can be found at: Harefield Primary School - Policies

8. Storage and Retention

Recorded data will not be retained for longer than 30 days except where the image identifies an issue and is retained specifically in the context of an investigation of that issue.

The data will be stored securely at all times, and in line with the retention as above. If storage is online, we will ensure that the storage locations are within the UK, and is encrypted. The data will be erased permanently and securely once there is no reason to retain the recorded information. Any physical matter (e.g. tapes or discs) will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

9. Subject Access Requests

- Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act 2018 and the GDPR.
- All requests should be made in writing to the School Data Compliance Officer or Trust Data Protection Officer (please see the Data Protection Policy for contact details).
- Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified, for example, a date, time and location.
- The school will respond within one calendar month from the date of the written request.
- The school may not have a facility to provide copies of CCTV footage but instead the applicant may be invited into the school to view the CCTV footage if available.
- If the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and the images pixelated so that only the person requesting access can be identified. The school will attempt to conceal any other individuals digitally, however if it is not possible to conceal the identify of others, disclosure may be refused.
- The school may refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.
- Data subjects also have the right under GDPR to object to processing which includes the use of CCTV. If the school receives an objection, it will be dealt with in accordance with the school's data subject requests process.

10. Requests for Access and Disclosure of Images from Third Parties

- There will be no disclosure of recorded data to third parties other than authorized personnel such as the Police where it is necessary to access to the data (e.g. investigators).
- Requests for access should be made in writing to the School Leader or School Data Compliance Officer.
- The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

11. Freedom of Information

The school is a public authority for the purposes of the Freedom of Information Act 2000. The school may receive requests for a copy of recorded information under the FOIA. The school will deal with any FOI requests relating to its use of CCTV in accordance with its existing FOI policy and procedure.

12. Complaints/Concerns

- Any complaints or concerns in respect of the system's use, or regarding compliance with this policy, should be addressed to the School Leader and investigated by the School Leader.
- If an issue remains unresolved, complainants should follow the school Complaints Policy and Procedure.

13. Review

The school's use of CCTV will be reviewed every year to ensure that their use remains necessary and appropriate, and that any CCTV used is continuing to address the needs that justified its introduction.

This policy will be reviewed annually and updated as required.

14. Related Policies and Procedures

- Data Protection Policy and Procedure
- Complaints Policy and Procedure
- Freedom of Information Policy

15. APPRENDIX 1

The 12 guiding principles from the Surveillance Camera Code of Practice:

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.