HILBRE HIGH SCHOOL
HUMANITIES COLLEGE

CCTV SYSTEM
POLICY

Author: Jane Whisker
Written: October 2022

Introduction:

CCTV has a legitimate role to play in helping to maintain a safe and secure environment for our staff, students and visitors. This policy is intended to address any concerns individuals may have regarding privacy. At Hilbre High School, we take our responsibility towards the security and safety of students, staff, visitors and school assets very seriously. We will use CCTV to monitor any instances of aggression, physical damage or theft to our school and its members.

The purpose of this policy is to manage and regulate the use of the CCTV systems at our school. To this end we are required to comply with Data Protection Legislation and we must ensure the CCTV images are useable for the purposes we require them for.

The policy covers the use of CCTV systems which capture moving and still images of people who could be identified. The captured images observe what individuals are doing and may be used to take action to prevent a crime.

This policy covers all employees, workers, contractors, agency workers, consultants, directors, members, trustees, past or present students and may also be relevant to visiting members of the public. The policy will be reviewed every 2 years, or sooner if new legislation or regulation comes into force.

The school will only use surveillance cameras for the safety and security of the school and its staff, students and visitors. The CCTV will be used as a deterrent for unacceptable behaviour and damage to the school.

1. Definitions:

1.1 For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage.
- Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.
- Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

1.2 Hilbre High School will only use covert surveillance in exceptional circumstances, for example, when required to by a police force.

1.3 CCTV cameras will be clearly signposted around the school.

1.4 For the purposes of this policy, the following terms have the following meanings:

CCTV means fixed and domed cameras designed to capture and record images of individuals and property.

Data is information which is stored electronically or in certain paper-based filing systems and may include Personal Data. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

Data Controllers means the person or organisation that determines when, why and how to process Personal Data.

Data Processors means the person or organisation that processes Personal Data on our behalf and in accordance with our instructions.

Data Users are those of our employees whose work involves Processing Personal Data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Privacy Standard and Privacy policy.

Data Subjects means a living, identified or identifiable individual about whom we hold Personal Data as a result of the operation of our CCTV (or other surveillance systems).

Personal Data means any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This will include video images of Data Subjects.

Processing means any activity that involves the use of Personal Data. It includes obtaining, recording, holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it.

2. The data protection principles:

2.1 Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Objectives:

3.1 The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of students, staff and visitors.

- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

4. Protocols:

4.1 The surveillance system will be registered with the ICO in line with data protection legislation.

4.2 Appropriate signage is placed throughout the school where the surveillance system is active.

4.3 The CCTV cameras will not be trained on individuals unless an immediate response to an incident is required.

4.4 The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

5. Security:

5.1 Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

5.2 The main control facility is kept secure and locked when not in use.

5.3 The CCTV systems will be tested for security flaws termly to ensure that they are being properly maintained at all times. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

5.4 Visual display monitors should be located in designated areas.

6. Code of practice:

6.1 The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

6.2 The school notifies all students, staff and visitors of the purpose for collecting surveillance data via notice boards, privacy notices, letters and emails.

6.3 CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

6.4 The CCTV system is for the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.

6.5 The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

6.6 The school will ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website.

6.7 The CCTV system will be designed to take into account its effect on individuals and their privacy. It will be used in a transparent way and will have appropriate signage associated with it.

6.8 There must be clear responsibilities and accountabilities for images and information collected, held and used. The CCTV policy should be communicated throughout the school. Images should only be retained for as long as required and access should be restricted to key personnel.

7. Access:

7.1 Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed. They have the right to submit a Subject Access Request for CCTV images of themselves.

7.2 All images belong to, and remain the property of the school.

7.3 Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher, who will consult the DPO, on a case-by-case basis.

7.4 It is important that access to, and disclosure of, the images recorded by CCTV is carefully controlled to ensure that the rights of individuals are preserved, and also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

7.5 Requests for access or disclosure will be recorded and the Headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

8. Monitoring and review:

8.1 This policy will be monitored and reviewed every two years by the DPO and the Headteacher to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

8.2 The Headteacher will communicate changes to this policy to all members of staff.

8.3 The scheduled review date for this policy is October.