CCTV Policy

Policy Owner Sandeep Athwal

Full Name	Position	Signature	Date	Review Cycle
Sandeep Athwal	Director		01.01.2024	Annual

Contents:

Statement of intent

1. Legal framework

2. The data protection principles

3. Objectives

4. Protocols

5. Security

6. Privacy

7. Code of practice

8. Access

9. Monitoring and review

Statement of intent

At 'School of Coding', we take great responsibility to ensure the safety of Pupils, Staff and Visitors. To enable this, the use of CCTV *(closed-circuit television)* to monitor the members of our school is fundamental.

The purpose of this policy is to manage and regulate the use of the CCTV system at the School of Coding and ensure the following:

• *We comply with data protection legislation, including the Data Protection Act 1998 and General Data Protection Regulation (GDPR) which came into effect 25th May 2018*

• *The images that are captured are usable for the purposes required*

• *We assure those persons whose images are being captured, are being handled in accordance with data protection legislation and the GDPR principles (Accuracy, Storage Limitation, Integrity and Confidentiality (Security) and Accountability).*

This policy covers the use of CCTV and other systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

• *Observing what an individual is doing*

• *Taking action to prevent a crime*

• *Using images of individuals that could affect their privacy*

1. Legal framework

1.1   In producing this policy, due regard has been given to the following, but not limited to;

UK General Data Protection Regulation

Data Protection Act 2018

Freedom and Information Act 2000 (FOIA)

Health and Safety at Work Act 1974

The Management of Health and Safety at Work Regulations 1999

The Children's Act 1989

The Children's Act 2004

The Equality Act 2010

1.2   This policy will also have regard to the following statutory and non-statutory guidance:

Safeguarding

Surveillance Camera Code of Practice

Data Protection Policy

UK General Data Protection Regulation

Data Protection Act 2018

Alternative Education Provision

Freedom and Information Act 2000 (FOIA)

2. The data protection principles

2.1   Data collected from 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 CCTV system will be used to:

    • Maintain a safe environment.
    • Ensure the welfare of pupils and staff.
    • Deter criminal acts against persons and property.
    • Assist the police in identifying persons who have committed an offence.

4. Protocols

4.1 Warning signs have been placed throughout the premises to notify people that CCTV system is active

4.2 The CCTV system has been designed for maximum effectiveness and efficiency; however, the School of Coding <u>cannot</u> guarantee that every incident will be detected or covered and 'blind spots' may exist.

5. Security

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

5.2 The school's authorised CCTV system operators are:

• CEO
• Director
• Operations Manager
• Senior Administrator

5.3 CCTV systems will be properly maintained accordingly

6. Privacy

6.1 Live and recorded materials will only be viewed by authorised operators for the purpose of investigating incidents.

6.2 Images may be released to the police for the detection of crime in line with data protection legislation.

6.3 Viewings of images by the police will be recorded by the School of Coding in a log.

6.4 Images will only be retained for as long as they are required.

6.5 Data protection impact assessments will be conducted for any new CCTV systems implemented in the school.

6.6 In the event of a data breach, the School of Coding appointed person will report the breach to the ICO within 72 hours if required to do so, as outlined in data protection legislation.

7. Code of practice

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

7.2 The School of Coding notify all persons attending the site via display notices.

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

7.4 All CCTV footage will be kept for 2 weeks for security purposes; the Operations Manager is responsible for keeping the records secure and allowing applicable access.

7.5 The school has a CCTV surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

7.6 The CCTV system is owned by the School of Coding and images from the system are strictly controlled and monitored by authorised personnel only.

7.7 The School of Coding will ensure that the CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

8. Access

8.1 Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

8.2 All discs containing images belong to, and remain the property of, the School of Coding.

8.3 Individuals have the right to submit an SAR *(Subject Access Request)* to gain access to their personal data in order to verify the lawfulness of the processing

8.4 The School of Coding will verify the identity of the person making the request before any information is supplied.

8.5 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information

8.6 Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

8.7 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

8.8 All requests will be responded to without delay and at the latest, within one month of receipt.

8.9 In the event of numerous or complex requests, the period of compliance will be extended by a maximum of a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

8.10 Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

8.11 In the event that a large quantity of information is being processed about an individual, the School of Coding will ask the individual to specify the information the request is in relation to.

8.12 It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

8.13 Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:
• The police – where the images recorded would assist in a specific criminal inquiry
• Prosecution agencies – such as the Crown Prosecution Service (CPS)
• Relevant legal representatives – such as lawyers and barristers
• Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

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

9. Monitoring and review

9.1 The CEO in collaboration with the Head of Operations will be responsible for reviewing the policy annually.

9.2 The Head of Operations will be responsible for monitoring any changes in legislation which may affect this policy and make the appropriate changes accordingly.

9.3 Any changes made to the policy will be circulated accordingly.