CCTV Policy

Policy approval date	29.06.2021
Policy review date	June 2023
Policy Lead	Data Protection Officer
Trustee approval	Trustee Approval
Committee responsible for policy	Trust Standards Committee

Introduction

This policy covers the use of CCTV and access to CCTV data.

As an organisation, we believe that the use of CCTV can play a legitimate part in creating and maintaining a safe and secure environment for students, staff and visitors. However, we acknowledge that the use of CCTV carries privacy and data protection implications and the impact on the rights of data subjects. This policy sets out our commitment to complying with our legal obligations and ensuring that the rights of data subjects are respected.

The controller and operator of the CCTV scheme are:

Controller: Clarion Academy Trust
Telephone: 01508 520359
Address: Kittens Lane, Loddon. NR14 6JU

Day-to-day management responsibility for deciding what information is recorded, how it is used and who can access it is delegated to the Trust Estates Manager.

Data Protection Officer: Data Protection Education Ltd.
Contact email: dpo@dataprotection.education
Telephone: 0800 0862018
Address: Unit 1 Saltmore Farm, New Inn Rd, Hinxworth, Hertfordshire, SG7 5EZ

Data Protection Education Ltd

Principles

Closed circuit television (CCTV) is a self-contained surveillance system comprising of cameras, recorders and displays for monitoring activities around our school sites. It is used in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 as set out in the Data Protection Bill.

This policy is guided by the Surveillance Camera Commissioner's Code of Practice (as required under the Protection of Freedoms Act 2012) which state:

System operators should adopt the following 12 guiding principles:

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.

Purpose

We use CCTV in and around our sites only for legitimate purposes. These are:

- for the safety and security of students, staff and visitors
- to protect buildings and assets from damage, disruption, vandalism and other crime
- to support law enforcement bodies in the prevention, detection and prosecution of crime
- to assist in the defence of any civil litigation, including employment tribunal proceedings

Cameras are used for both recordings of data and live monitoring. It is rarely used for live monitoring but where live monitoring is available, we take steps to ensure that there is controlled access to live monitors to authorised members of staff only.

Location of Cameras

Cameras will only be located in positions that are required for the identified purposes. CCTV cameras will be positioned or masked to prevent monitoring and recording of any external private property.

Examples of locations where CCTV monitors 24 hours a day, 7 days a week include the entrance to the school site and school reception.

Notices

Use of CCTV will be referenced in the Organisation's Privacy Notices and in a privacy statement available to visitors at the reception.

Signage is displayed at all points of entry on site and at points of entry into areas where cameras are present.

Signage will be clear and include:

- Name of the system operator
- Purpose of the system
- Contact details

An example CCTV sign is included in Appendix A.

Retention

Data will be kept no longer than necessary, after which is automatically deleted permanently. No backups are available. Our standard retention period is up to 30 days. Data may be kept for longer periods for any on-going investigations. This will be securely disposed when the investigation reaches a conclusion.

Where the data is extracted and required for other legal purposes (e.g. investigation of a crime), data will be kept as long as required for that purpose. Each instance will be logged in the CCTV extraction log.

Any redundant hardware will be destroyed securely.

Security and Maintenance of CCTV Equipment

IP and network cameras

Physical CCTV equipment must be kept in a secure location. Any standalone CCTV recorders/storage device must be permanently stored in a secure location or housing unit.

Where cameras are accessible over a network, penetration testing of this network should take place on a minimum annual basis. Any organisations processing this data on the Organisation's behalf must do so under the explicit instructions of the data controller.

All cameras and equipment will be checked weekly to ensure they are operating correctly.

Access to CCTV Data

Access to CCTV images is limited to authorised staff only. Images can only be used in support of a defined legitimate purpose and not for any other routine purpose. Details of CCTV processes at Clarion schools are outlined in a separate flowchart document. Authorised staff must sign a CCTV authorised staff agreement (code of practice) prior to being able to access CCTV images.

When access is requested and is to be viewed by anyone other than the delegated person responsible, it must be authorised by the delegated authority and documented in the CCTV Access Log. Any CCTV footage will be viewed in a secure location.

Exemptions, as described in the ICO guidelines may be applied to any data disclosure.

In Criminal Proceeding

CCTV data will be disclosed to the Police or other agencies only where a clear legal obligation to do so has been identified and appropriate documentation (usually a Disclosure Request Form provided by the requesting agency) received under Schedule 2, Part 1 Paragraph 2, of the Data Protection Act 2018 (previously S29 of the Data Protection Act 1998).

Once this information has been disclosed it is noted that the receiving party becomes the data controller.

By Third-Parties (Subject Access Requests)

Data subjects may ask for copies of their data under their right of access under the Data Protection Act 2018 and will be handled as per the Subject Access Request Procedure.

Where a request for CCTV data made, we require information on the time, date and place of the images.

Information may be provided as still images or video, with or without redaction as deemed necessary. On occasions, requests may be actioned by asking the data subject to view the data directly.

Misuse

Misuse of CCTV data will be a disciplinary matter and may also constitute a criminal offence.

Data Privacy Impact Assessments

We adhere to the following statement from the Surveillance Camera Commissioner:

- Principle 2 of the surveillance camera code of practice states that the use of a surveillance camera system must take into account the effect on individuals and their privacy, with regular reviews to ensure its use remains justified. The best way to ensure this is by carrying out a data protection impact assessment (DPIA) before any surveillance camera system is installed, whenever a new technology or functionality is being added on to an existing system, or whenever there are plans to process more sensitive data or capture images from a different location. This will assist in assessing and mitigating any privacy issues linked to the use of a surveillance system.

- A DPIA is one of the ways that a data controller can check and demonstrate that their processing of personal data is compliant with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. There are statutory requirements to carry out a DPIA in Section 64 DPA 2018 and article 35 of the GDPR.

A DPIA is mandatory where processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35). It is particularly relevant when new processing or new technology is being introduced.

In relation to CCTV, due to the systematic monitoring of data subjects, a risk assessment of the CCTV processing should be carried out in conjunction with the Data Protection Officer, following which a full DPIA may be required in order to help compliance with Data Protection Law.

Covert Surveillance

Covert monitoring (where the individual is not aware the monitoring is taking place) will only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity or extremely serious malpractice. Any covert surveillance will be legally reviewed and safeguards put in place prior to commencing.

Policy and CCTV review

CCTV, including this policy, associated logs and data privacy impact assessments will be reviewed annually by the organisation and the Data Protection Officer.

Appendix A: Example CCTV signage

Appendix B: CCTV access, extraction and approval flow

This flowchart is intended as a guide information flow to ensure that CCTV access and extraction occurs only when both these conditions are met:

- a prior incident exists (where that incident type is documented as a purpose of the CCTV in the organisation's CTV Policy) and is recorded as an incident
- when authorised by the appropriate personnel

Incident reporting policies should document the threshold for incident severity.

The CCTV policy should define authorising personnel and those with access to view and extract data from the CCTV system.

Security measures for storage and deletion to be documented in the CCTV policy.