Stoke Holy Cross Primary School

CCTV Policy

[Version v1.5]

If you would like to discuss anything in this privacy notice, or if you would like a copy, please contact the school office: **office@stokeholycross.norfolk.sch.uk**

Document Version

Version	Author	Date	Approved by	Effective from
1.0 template	DPE	1 January 2019		
1.1	DPE	10 June 2019		
1.2	DPE	23 November 2020		
1.3	DPE	07 October 2022		
1.4	DPE-VH	12/08/24		
1.5		01.09.26		

Contents

Introduction 6

Principles 6

Purpose 7

Location of cameras 8

Notices 8

Retention 8

Security and maintenance of CCTV Equipment 9

IP and network cameras 9

Access to CCTV data 9

In Criminal Proceeding 9

By Third-Parties (Subject Access Requests) 9

Misuse 10

Data Privacy Impact Assessments 10

Covert Surveillance 11

Policy and CCTV review 12

Appendix A: Example CCTV signage 13

Appendix B: CCTV access, extraction and approval flow 14

DPE TEMPLATE - Disclaimer 16

Reference documents:

- Information Commissioner's Office CCTV Code of Practice
- Surveillance Camera Commissioner Code of Practice
- Protection of Freedoms Act 2012
- Data Protection Act 2018

Associated documents:

- CCTV Log
- CCTV Systems Log
- CCTV Access Log

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: Stoke Holy Cross Primary School

Contact email: office@stokeholycross.norfolk.sch.uk

Telephone: 01508493132

Address: Long Lane, Stoke Holy Cross, Norwich NR14 8LY

Day-to-day management responsibility for deciding what information is recorded, how it is used and who can access it is delegated to **Headteacher – Miss J Chaney**

Day-to-day responsibility for operational maintenance of the cameras and security of the equipment has been delegated to **Headteacher – Miss J Chaney**

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

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

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:

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

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

The CCTV system will NOT be used:

A. to record sound unless in accordance with the policy on covert surveillance (see below);
B. for any automated decision taking; or
C. monitoring private and/or residential areas or premises.

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.

CCTV monitors the following locations 24 hours a day, 7 days a week:

A. Points of entrance onto the site
B. Points of entrance into the building
C. Playgrounds and carparks

We will make every effort to position cameras to ensure they only cover our premises.

Cameras will not focus on residential or private accommodation or property. Where this is not possible, we will use physical or electronic masking to prevent unnecessary recording and intrusion. Any stakeholders should be consulted as part of a data protection impact assessment prior to the deployment or change to the CCTV in these circumstances.

Camera operators will receive training and access to written procedures for maintaining and respecting the privacy of neighbours (business and residential), staff and customers.

With the exception of covert monitoring, cameras will not be hidden from view and must be sited in such a way as to ensure that they only monitor spaces intended to be covered.

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 15 days.

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.

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 and

All cameras and equipment will be checked weekly to ensure they are operating correctly. These checks will be recorded in the CCTV Systems Log.

Access to CCTV data

Access to CCTV images can only be used in support of a defined legitimate purpose and not for any other routine purpose.

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. Wherever possible, a minimum of two authorised people should view the footage.

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 Proceedings

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 is 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 comply with Data Protection Law.

A DPIA should also be conducted prior to any installation, for any purpose where artificial intelligence, or automated processing is used.

Covert Surveillance

Covert monitoring will not normally be considered. In exceptional circumstances, covert surveillance using CCTV may be carried out in a manner where those subject to it are unaware it is taking place.

The organisation understands that covert surveillance is rarely justified and is in contravention of the third principle of the ICO CCTV Code of Practice:

> "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. "

Therefore covert surveillance is only permissible for the following purpose:

- Where the surveillance is required for investigating a crime or equivalent malpractice, when notifying individuals about the monitoring would prejudice its prevention or detection

In order for covert surveillance to be permitted the following safeguards must ALL be adhered to, fully documented and approved:

- **Agree scope and process.** The surveillance scope should define the following:
  - **Purpose of the processing with justifications**
  - **Time-limitation.** The duration should be defined in advance and the surveillance stop as soon as the investigation is completed
  - **Data subjects being surveilled** (the surveillance may be illegal if non-targets are covered by the surveillance)
  - **Location and coverage. T**here will be no covert surveillance in a private space, including private offices or toilets
  - **Disclosure.** Rules on who and when can access the data will be defined in advance
- **Balancing test:** once the scope is defined the Organisational Leadership will conduct a balancing test
  - Define and document the reasons why the surveillance needs of the organisation outweigh the rights of the data subject in question
- **Data Protection Impact Assessment**
  - The DPO shall complete a DPIA prior to any deployment
- **Legal Review**
  - The scope, balancing test and DPIA should be verified by the organisation's legal counsel to ensure the organisation will not be conducting illegal processing

Use of data. Any unrelated data (unless it reveals information that cannot reasonably be ignored) will be disregarded and where possible deleted.

Private Investigators will only be used with a defined contract that meets all the required of the Data Protection Act 2018 including to only collect and use data that is required and clauses to ensure data confidentiality and security

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

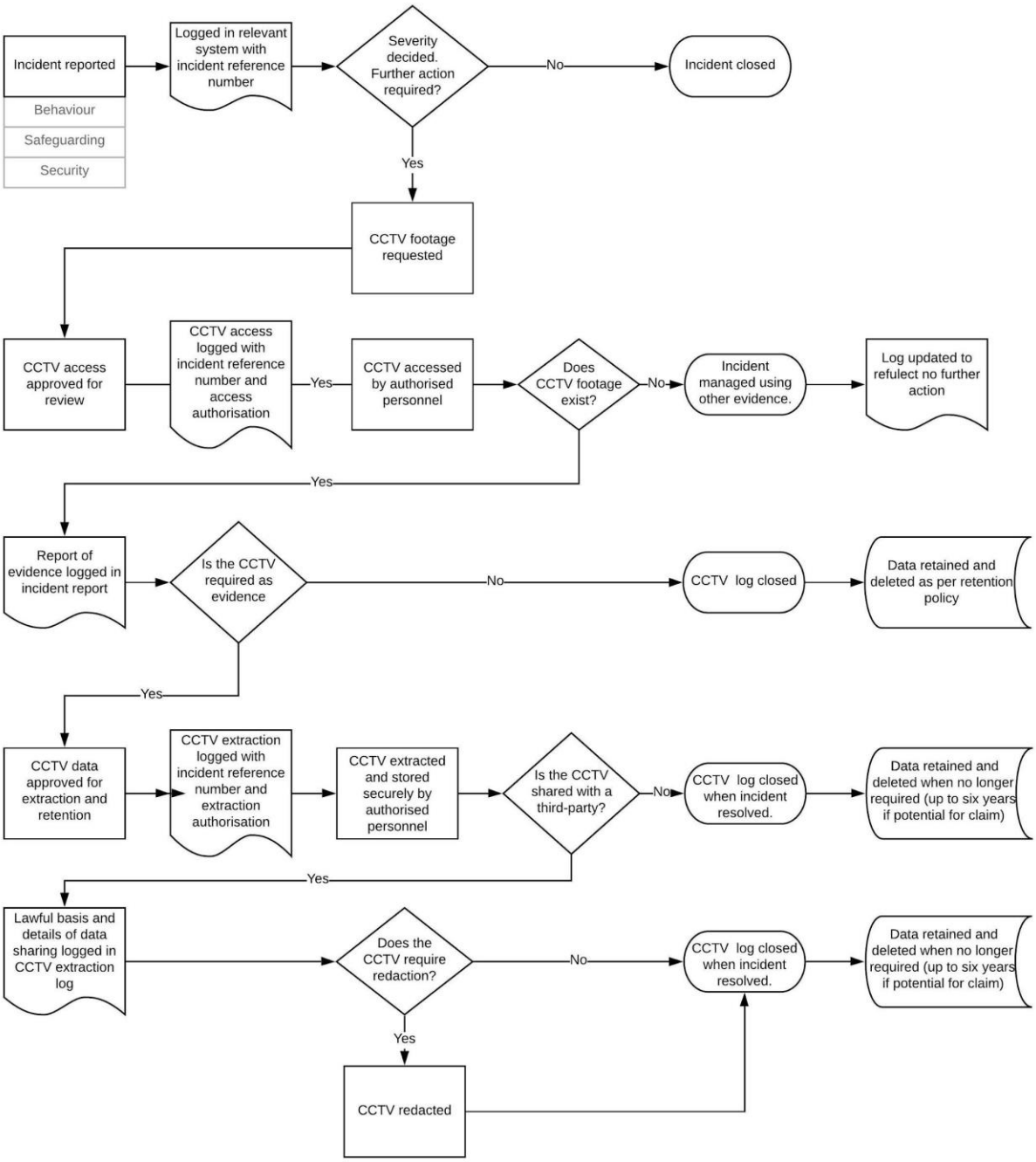
This flowchart is intended as a guide information flow to ensure that CCTV access and extraction occurs only when both these conditions are met:

- a prior incident exists (where that incident type is documented as a purpose of the CCTV in the organisation's CCTV 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.


Incident reported
Behaviour
Safeguarding
Security
Logged in relevant system with incident reference number
Severity decided. Further action required?
No
Incident closed
Yes
CCTV footage requested
CCTV access approved for review
CCTV access logged with incident reference number and access authorisation
Yes
CCTV accessed by authorised personnel
Does CCTV footage exist?
No
Incident managed using other evidence.
Log updated to refulect no further action
Yes
Report of evidence logged in incident report
Is the CCTV required as evidence
No
CCTV log closed
Data retained and deleted as per retention policy
Yes
CCTV data approved for extraction and retention
CCTV extraction logged with incident reference number and extraction authorisation
CCTV extracted and stored securely by authorised personnel
Is the CCTV shared with a third-party?
No
CCTV log closed when incident resolved.
Data retained and deleted when no longer required (up to six years if potential for claim)
Yes
Lawful basis and details of data sharing logged in CCTV extraction log
Does the CCTV require redaction?
No
CCTV log closed when incident resolved.
Data retained and deleted when no longer required (up to six years if potential for claim)
Yes
CCTV redacted

DPE TEMPLATE - Disclaimer

Please note that your use of and reliance on this document template is at your sole risk and should be used as a starting point only, from which you will ensure that the content of any document you create is correct and appropriate for your needs and complies with relevant laws in your country. You should take all reasonable and proper legal and other professional advice before using this document. DPE disclaims liability for any cost, expense, loss or damage suffered or incurred in reliance on our document templates, or in expectation of our document templates meeting your needs, including (without limitation) as a result of misstatements, errors and omissions in their contents.