NORTH NEWTON COMMUNITY PRIMARY SCHOOL
CCTV POLICY
including
BODY-WORN VIDEO AND SURVEILLANCE

Contents

Contacts and Review Information

Data Protection Officer dposchools@somerset.gov.uk

School Data Protection Lead DEBORAH LEACH

The policy was approved by Governors / Trustees on: 22/05/2023

Signature of Chair of Governors / Trustees: 

The next review date is: 22/05/2025

Version Control

Version	Author(s)	Date Produced	Amendments
1.0	Amy Brittan	10/03/20	Rewrite of eLIM CCTV Policy 2018
1.2	Amy Brittan	29/05/20	Minor textual changes. Additional information added to Section 13: Subject Access Requests.
1.3	Amy Brittan	06/01/21	Updated for post-Brexit legislation
1.8	Amy Brittan	23/09/22	Checked for any updates – removed ICO code of practice reference and updated link to Surveillance code

Introduction

1.1. At North Newton School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.

1.2. The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the UK GDPR, effective 1st January 2021.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation and their rights are being upheld.

1.3 This policy covers the use of surveillance and CCTV 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

About this policy

2.1 This policy has been created with regard to the Home Office guidance 'The Surveillance Camera Code of Practice' (2013, updated 2021)

2.2 This policy has due regard to legislation including, but not limited to, the following:

- The UK General Data Protection Regulation
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Protection of Freedoms Act 2012
- The Regulation of Investigatory Powers Act 2000

2.3 This policy operates in connection with the following school policies:

- Data Protection and Freedom of Information Policy

Definition of data protection terms

3.1 For the purpose of this policy a set of definitions will be outlined, in accordance with the Surveillance Camera Code of Practice:

- **CCTV** – Closed Circuit Television is a system of cameras which stream an image to a central monitor, where activity can be recorded.

- **Body-Worn Cameras (BWC)** – if felt appropriate, a camera worn by a representative of the school to capture video recordings. BWC are only activated when there is an incident.

- **Surveillance** – monitoring the movements and behaviour of individuals; through CCTV or BWC.

- **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. The school does not condone the use of covert surveillance when monitoring staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

The Data Protection Principles and Privacy by Design

4.1 Data collected from surveillance and CCTV will be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date;
5. Kept for no longer than is necessary for the purposes for which the personal data are processed;
6. 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.

4.2 The school will follow the ICO's guidelines on Privacy by Design – before planning installing and using a surveillance system, the school will:

- Consider whether the school can fulfil its requirements through a less privacy-intrusive system that does not include surveillance and recording.
- Carry out a Data Privacy Impact Assessment (DPIA) to assess security risks and how the rights of individuals will be upheld. A copy of the DPIA is appended to this policy.
- Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

Responsibilities of the School

5.2 The school, as the corporate body, is the data controller. The governing board of school therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

5.3 The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure.

Responsibilities of the Data Protection Officer

6.1 As a school we are data controllers in law and are required to appoint a Data Protection Officer. Our DPO is Amy Brittan and can be contacted at dposchools@somerset.gov.uk

6.2 The DPO is responsible for ensuring compliance with current Data Protection legislation and with this policy. Their responsibilities are laid out in the Data Protection policy, but in relation to CCTV and surveillance they include:

- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with the 6 data protection principles.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Supporting the school to complete a Data Privacy Impact Assessment when installing or replacing cameras (see paragraph 4.2).
- Reviewing the effectiveness of the current CCTV system and making recommendations if appropriate.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school; their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.

Responsibilities of the headteacher

7.1 The headteacher has the following responsibilities:

- Meeting with the DPO to decide where CCTV or BWC is needed to justify its means.
- Liaising with the DPO regarding the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.
- Communicating any changes to legislation to all members of staff.

Purpose and justification

8.1 The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.

8.2 Surveillance will be used as a deterrent for violent behaviour and damage to the school.

8.3 The school may share surveillance footage to assist the police in identifying persons who have committed an offence (see paragraph 13.1).

8.4 The school will only conduct surveillance as a deterrent and will not site cameras in classrooms or any changing facility.

8.5 The school may use surveillance data as part of disciplinary and grievance processes. This will be communicated to students and staff through the school's Privacy Notices.

8.6 If the surveillance and CCTV systems do not fulfil their purpose and are no longer required the school will deactivate them.

How the School manages CCTV and surveillance

9.1 The school is registered as a data controller with the Information Commissioner's Office, which also covers the use of surveillance systems.

9.2 CCTV warning signs are clearly and prominently placed at all external entrances to the school, including gates if coverage includes outdoor areas. The signs contain details of the purpose for using CCTV e.g. public safety or crime prevention.

9.3 In areas where CCTV is used, the school ensures that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

9.4 If BWC are being used, the staff member wearing the device will receive training on their appropriate use. They will only start recording when there is an incident they judge should be captured. They will display information which explains that they are wearing a camera and will clearly explain to the data subjects that they have started recording. Only trained and designated staff members will use BWC.

9.5 The surveillance system is a closed digital system will not record audio by default., as audio recording may be considered an excessive intrusion of privacy. If audio recording is possible, this option will be turned off.

9.6 The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

9.7 The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

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

Security

10.1 Access to the surveillance system, software and data is strictly limited to authorised school staff and is password protected.

10.2 The school's authorised CCTV system users are:
- Deborah Leach, headteacher.
- Claire Larcombe, office administrator

10.3 A Visual display monitor is located in the main office. The monitor screen is not in sight of the general public and is turned off when there is no requirement to view live images.

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

10.5 Surveillance and CCTV systems will be tested for security flaws once a term to ensure that they are being properly maintained at all times.

10.6 The headteacher and authorised staff will decide when to record footage, e.g. a continuous loop outside the grounds to deter intruders.

10.7 Any unnecessary footage captured will be securely deleted from the system.

10.8 Any cameras that present faults will be repaired immediately to avoid any risk of a data breach.

Covert monitoring

11.1 The school may in exceptional circumstances set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

11.2 In these circumstances authorisation must be obtained from a member of the senior leadership team.

11.3 Covert monitoring must cease following completion of an investigation.

11.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

11.5 The Human Rights and Employment Rights of all the people who use the school must be respected and covert monitoring must only be used as a last resort.

Storage and retention of images

12.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

12.2 The CCTV images will be kept for 60 days (in line with the purpose for recording this data) unless there is a current incident that is being investigated;

12.3 BWC images will be kept for 60 days (in line with the purpose for recording this data) unless there is a current incident that is being investigated;

12.4 All retained data will be stored securely and will be listed on the school's Data Asset Audit.

12.5 All retained data must be stored in a searchable system. Only a primary copy should be kept, and secondary copies should only be created in exceptional circumstances.

Subject Access Requests (SARs)

13.1 Individuals have the right to request access to video footage relating to themselves under the Data Protection Act 2018.

13.2 All requests should be made to the Headteacher or the Data Protection Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location. Requests may be written or verbal.

13.3 The school will immediately indicate receipt and then respond within one calendar month of receiving the request.

13.4 The school reserves the right to refuse access to video footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

13.5 All attempts will be made to allow the viewing of the video. If others can be identified, the school will assess the risk to others from the video being viewed by the requester. If there is likely to be a risk of harm, the school may consider the following options where appropriate:

- Obtain the consent of others to share the video with the requester;
- Use video-editing software to blur the faces of others who can be identified from the video;
- Provide selected still images from the video and blur the identifiable faces;
- Provide a transcript or written description of the contents of the video.

13.6 If all options have been considered and the school still consider there to be a risk to others from the requester viewing the video, the school may decline the request to view the video (although relevant exemptions in the Data Protection Act 2018 will need to be identified by the school provided to the requester).

13.7 The school should not provide copies of the video to others unless instructed to do so in law or there is no risk to individuals who may be identifiable from the video.

Access to and disclosure to other third parties

14.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators) and with the correct authorisation.

14.2 Requests from third parties should be made in writing to the Headteacher/Governing Body or the Data Protection Officer. However, consideration must also be given to the following paragraph (14.3)

14.3 Consideration should always be given to the safeguarding and best interest of pupils. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All disclosures and the reasons for release should be recorded.

14.4 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. This will be communicated to staff through the school’s Privacy Notices.

Complaints

15.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher/Governing Body or the Data Protection Officer in the first instance.

Appendix 1 - Privacy Impact Assessment (PIA) for CCTV

Data Protection Principles

- processing to be lawful and fair
- purposes of processing be specified, explicit and legitimate
- adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is necessary
- processed in a secure manner

Why we need a Privacy Impact Assessment – screening questions

We need to complete this form because:

- we are using new technology that might be perceived as being privacy intrusive e.g. the use of biometrics or facial recognition; (CCTV)
-

Describe the service
North Newton Community Primary School) is using closed circuit television (CCTV) and the images produced to prevent or detect crime and to monitor the school buildings and grounds in order to: • provide a safe and secure environment for pupils, staff and visitors, • prevent loss or damage to school property.

Adapted from https://ico.org.uk/media/for-organisations/documents/1042836/pia-code-of-practice-editable-annexes.docx

CCTV is not a requirement of the school's insurance policy but is a recommendation from our insurers.

The lawful basis for the use of the CCTV system is Article 6(1)(f) of UK GDPR: Legitimate Interests of the Data Controller. In using this as our lawful basis, we have assessed:

- **Purpose:** the processing fulfils a clear function - indicating possible criminal acts or threats to the security of pupils/staff/visitors (the public)
- **Necessity:** we consider that the CCTV system is the only reasonable way to meet this objective, and we have ensured that it is processed with as little intrusion into the privacy of individuals as possible
- **Balancing:** We recognise that this data processing may be considered sensitive, but we have taken measures to minimise the negative impact on individuals by pointing fixed cameras at the school gates only and not at public space. No audio is recorded on the CCTV throughout the site.

Describe the data collected and the possible uses of the data

List of data held	**Collection of data**

Any user or visitor to the main school site could be captured on the CCTV system, this could include; pupils, parents, staff, visitors, contractors etc	• There are currently 2 CCTV cameras at these locations:
	  ○ Fixed to the main school building and capturing images of the entrance gate on the Church Road side of the premises
	  ○ Fixed to the main school building and capturing images of the main entrance gate of the premises.
	• Cameras will capture video footage and still images
	• No audio will be captured
	• All cameras are fixed
	• All data is stored securely on a separate CCTV recorder, access to which is password protected.
	• CCTV viewing equipment is held in the school office which is access controlled and access to the recordings is limited to the individuals outlined in the school's CCTV policy.

	• CCTV viewing equipment is secured by password, and access is only available to those outlined in the CCTV policy. • CCTV footage is configured to be retained for the retention period set out in our CCTV policy (60 days) and after this date it is overwritten.
	Possible uses • The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors. The cameras are used in conjunction with the school security access system to confirm identity of visitors requesting access to the school grounds. A monitor in the school office provides images of those waiting at the school gate prior to being allowed access by office staff. • Surveillance will be used as a deterrent for those wishing to enter the school grounds for malicious or criminal purposes and signage will be clearly visible. • The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in general classrooms or any changing facility. • If the surveillance and CCTV systems do not fulfil their purpose and are no longer required, the school will deactivate them.

Identify the privacy, related risks and possible solutions To be discussed with the Data Protection Lead			
Privacy issue	Risk to individuals	DPA Risks	Possible Solutions
Surveillance methods may be an unjustified intrusion on privacy.	Medium/High	Breach of principle 1 of UK GDPR – lawful, fair, transparent; principle 3 – data minimisation	Cameras are positioned so that they only cover areas of the school buildings and grounds. They do not cover any 'public or private space'. Monitoring of the school gates only takes place and access to CCTV footage will be restricted as outlined in our CCTV policy.
If a retention period is not established information might be used for longer than necessary.	Low	Breach of principle 5 of UK GDPR – storage limitation; principle 2 – purpose limitation	CCTV equipment configured to retain footage in line with CCTV policy (60 days). In the event of an incident that requires that footage is held for longer than this period, footage will be deleted as soon as the matter is concluded.
Access to the system by unauthorised parties (Hacking)	Significant	Breach of principle 6 of UK GDPR – security	All cameras to be hard cabled and system will require password to be entered to be accessible
Unauthorised Disclosure	Significant	Breach of principle 6 of UK GDPR – security	Internal guidance will be provided in the form of a CCTV policy – clearly states who data will be shared with and why.

			Privacy notices and signage will allow individuals to be informed of CCTV usage. No audio recording. Limited access to recordings. Retention is 60 days in the usual course of events. Only the Team outlined in the CCTV policy will have access to the system and all viewings will be logged. We will only share data with: • 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 where legal advice is sought • 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 • Staff with appropriate responsibility for completing formal investigations into serious breach of School rules.

Sign off and notes

Comments on risks	Processes that must be in place
Security flaws – cameras may malfunction or retain data longer than expected	Ensure proper maintenance and that cameras are checked termly to ensure necessary footage is still be recorded, and that old footage is being deleted
Signage may not be up to date	Data Lead to check that CCTV signage is still clearly visible on termly walks around the school
Access to footage may be given to unauthorised personnel	Data Lead and DPO must be consulted before any footage is shared with third parties - see CCTV policy

Contact point for future privacy concerns

Data Protection Officer: dposchools@somerset.gov.uk

Data Protection Lead: (Deborah Leach)

Date completed: 04/06/2023