# Milverton Community Primary and Pre-School - CCTV POLICY July 2022

## Contents

# Contacts and Review Information

Data Protection Officer dposchools@somerset.gov.uk

School Data Protection Lead r.stead@milvertonprimary.co.uk

The policy was approved by Governors / Trustees on: _____

Signature of Chair of Governors / Trustees: _____

The next review date is: _____

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 | Andy Wooller | 11/07/22 | Policy re-worded to reflect the specific use of CCTV at the School. |

# Introduction

1.1. At Milverton Community Primary and Pre-School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use CCTV cameras to monitor any instances of intrusion or physical damage to our School site and/or buildings.

1.2. The purpose of this policy is to manage and regulate the use of the CCTV systems at Milverton Community Primary and Pre-School and ensure that:

- We comply with the GDPR, effective 25 May 2018.
- 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 following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2014) 'CCTV Code of Practice'

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

- The General Data Protection Regulation 2016
- 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 Milverton Community Primary and Pre-School policies:

- Data Protection and Freedom of Information Policy

- Parents' consent for use of Imagery.
- CCTV Privacy Impact Assessment.

## 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)** - a camera worn by a representative of the School to capture video recordings. (BWC are currently not in use.)
- **Surveillance** – monitoring the movements and behaviour of individuals; through CCTV or BWC. Surveillance of any Pupils or Staff is not currently employed at Milverton Community Primary and Pre-School.
- **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. Milverton Community Primary and Pre-School does not condone the use of covert surveillance.

## 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.
- 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 the 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 with regard to 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 CCTV cameras for the security of the School site and buildings.

8.2 CCTV will be used as a deterrent for intrusions to, or damage to, the School site and/or buildings.

8.3 The School may share CCTV footage to assist the police in identifying persons who have committed an offence (see paragraph 14.1).

8.4 No cameras will be installed inside the School; the system is not intended to capture any Pupils or Staff, or other persons carrying out their legitimate business.

8.5 No recording will occur between the hours of 08.00 and 16.00.

8.6 If the surveillance and CCTV systems do not fulfil their purpose or 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 and 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. Where there is permitted public access through areas that are part of the School site, signs are placed to ensure that member of the public are aware of the possibility of being recorded.

# 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:

- Nicola Stoddart – Head Teacher.
- Marian Barlow – Office Manager.
- Andy Wooller – company that installed equipment

10.3 A Visual Display Monitor is located adjacent to the CCTV Recorder in a location to which pupils and visitors do not have access. The monitor screen is not in sight of the general public and is turned off when there is no requirement to view images.

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

10.5 A remote monitoring facility is enabled to allow maintenance of the system and to receive notifications of intrusions onto the School site when the School is closed. Use of this is restricted to the authorised CCTV systems users. Users undertake not to monitor any cameras during the School day.

10.6 Surveillance and CCTV systems will be tested for security flaws once a term to ensure that they are being properly maintained at all times. The remote monitoring facility allows the authorised users to be made aware of any faults in real time.

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

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

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

# Covert monitoring

11.1 The School does not use any covert monitoring and does not intend to do so.

# 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 are automatically overwritten once the storage capacity of the recorder is reached. The system has been designed with sufficient storage to retain images through the summer holiday period (in line with the purpose for recording this data) Images are thus automatically overwritten after approximately 2 months unless there is a current incident that is being investigated.

12.4 Any data retained for a specific purpose 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.

## 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.