The Castle Partnership Trust
ACHIEVE | BELONG | PARTICIPATE

CCTV Use Policy

Date: February 2022

CEO: Sarah Watson
Headteacher, The Castle School: James Lamb
Headteacher, Court Fields School: Polly Matthews
Headteacher, Wellesley Park School: Carly Wilkins
Headteacher, Isambard Kingdom Brunel and Orchard Grove Schools: Richard Healey

Due for review: Spring Term 2024

1. INTRODUCTION

1.1 The Trust has installed a CCTV system in its schools in order to protect against crime and to protect students, staff, parents and members of the public when they are on Trust premises. The systems comprise a number of fixed and dome cameras located around the school sites and are owned by the Trust.

1.2 This policy is to enable the Trust to comply with the Data Protection Act 1998, the General Data Protection Regulations (GDPR) and subsequent guidance released by the Information Commissioner's Office and under the Human Rights Act 1998.

1.3 This policy applies where open use of CCTV is intended in public areas. It does not apply to targeted or covert surveillance activities.

1.4 This policy will be reviewed as appropriate or as legal advice changes.

2. RESPONSIBILITIES FOR CCTV OPERATION

2.1 The CCTV scheme is administered and managed by the Headteacher and the Business/Premises/IT Managers in accordance with this policy and with guidance from the DFE where necessary.

2.2 The day-to-day management of the CCTV scheme is the responsibility of the SLT and the Business/Premises/IT Managers during the day and at evenings, weekends and during school holidays.

2.3 Precautions are in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to any guidance or security precautions.

3. LEGAL BASIS FOR USE OF CCTV SYSTEMS

3.1 The use of CCTV and the images recorded will comply with the Data Protection principles and will be:

- Fairly and lawfully obtained;
- Adequate, relevant and not excessive;
- Accurate;
- Used only for purposes about which people have been informed;
- Secure and protected from unauthorised access;
- Not held longer than required for the purposes for which they were recorded;
- Accessible to data subjects where a request has been made under the Data Protection Act and the GDPR, and where the images are defined as personal data.

3.2 The purposes for which CCTV is in use across the Trust are the following:

- Prevention and detection of crime, eg, theft, arson and criminal damage;
- To protect the Trust buildings and assets;
- To increase the perception of safety and reduce the fear of crime;
- To assist in the management of each school eg accessibility and condition of site in poor weather, behaviour of students when constant supervision is not possible;
- To protect members of the public and private property;
- To ensure the safety of students and others present on school Trust premises and enhance positive behaviour of students, staff and visitors.

- To provide evidence in insurance claims, legal cases, disciplinary investigations/hearings and grievance meetings/appeals.

3.3 The use of CCTV will be fair and not be excessive or prejudicial to any individual or any group of individuals. The Trust will inform people that CCTV is in use on the premises by means of notices.

3.4 Each school will document the purposes for which CCTV is to be used on the premises.

4. ENSURING THAT USE OF CCTV IS FAIR

4.1 The Trust will include the use of CCTV on its annual Data Protection notification (registration) to the Information Commissioner's Office as one of the purposes for which it uses personal data. The Trust will treat the system and all information, documents and recordings obtained and used as data which is protected by the Data Protection Act and the GDPR.

4.2 The Trust will only use CCTV for the purposes stated. CCTV or images produced from it will not be used for any other purposes, particularly purposes which could not reasonably be envisaged by individuals.

4.3 The Trust will ensure that students, staff and other people who use its buildings are informed of the use and purpose of CCTV. This will be done by means of clear and obvious notices placed around each school premises. Notices will include the following information:

- The identity of the Data Controller (the relevant school);
- The purposes for which CCTV is being used, eg, for the prevention or detection of crime or to increase safety and security whilst on Trust premises;
- Details of who to contact about the scheme and name/phone number where applicable.

4.5 CCTV cameras will only record images on Trust premises and will not be directed at surrounding private property.

4.6 A privacy impact assessment is in place for CCTV systems across the Trust. This is referred to when new cameras are installed and is reviewed along with the CCTV policy. (See appendix 1)

5. SECURITY

5.1 CCTV viewing access will be strictly confined to authorised staff. Where other staff or visitors need to have access to the system, this will be documented.

5.2 If out of hours emergency maintenance is required the staff member in charge of the CCTV system must be satisfied of the identity of contractors before allowing access to the equipment.

5.3 Remote access to cameras via 'off air' access or via broadband links will be used sparingly. When accessing cameras from home over the Internet, staff will ensure that unauthorised persons cannot view the footage.

Retention of recordings

5.4 Recordings will be held for a limited length of time and will be destroyed when their use is no longer required. The maximum period is normally 28 days but this may be extended where the recordings are required for an ongoing investigation. When the retention period has been reached, digital recordings or removable media will be destroyed or wiped securely.

6. COVERT SURVEILLANCE

6.1 On the rare occasions when the Trust may wish to use CCTV covertly (ie, without making people aware of it), an application will be made under the Regulation of Investigatory Powers Act (RIPA). The Trust will discuss the matter with its solicitors to ensure appropriate guidelines are followed.

6.2 Where the police wish to undertake covert surveillance, they will gain authorisation from their own Single Point of Contact (SPOC).

7. PROCEDURES FOR DISCLOSURE OF CCTV RECORDS TO OTHER ORGANISATIONS

7.1 Access to CCTV recordings day-to-day will be restricted to members of SLT, Business/Premises Managers and Heads of House/Pastoral Support Assistants (but only as directed by Heads of House).

7.2 CCTV recordings will be held only by the Trust unless there is a legitimate reason to disclose them. Disclosure includes the viewing of images by someone who is not the operator of the system as well as the transfer of recordings to another organisation.

7.3 Records may need to be disclosed for the following reasons:

- To students, parents, governors/directors or other staff when footage relates to behaviour management;
- To the police, for the prevention and detection of crime;
- To a court for legal proceedings;
- To a solicitor for legal proceedings;
- To the media for the purposes of identification.
- To insurers for an insurance claim, disciplinary investigation/hearing, grievance or appeals.

7.4 Where recordings have been disclosed or viewed by an authorised third party each school will keep a record of:

- When the images were disclosed;
- Why they have been disclosed;
- Any crime incident number to which they refer;
- Who the images have been viewed by or disclosed to.

7.5 Viewing of CCTV recordings by the Police will be recorded in writing. Requests by the Police are actioned under section 29 of the Data Protection Act and the GDPR. The Police should provide a completed section 29 form stating that the information is required for the prevention and detection of crime. If a form is not available, or in an emergency, the school must record in writing when and why the information has been released.

7.6 Should a recording be required as evidence, a copy may be released to the Police. Where this occurs the recording will remain the property of the Trust. The date of the release and the purpose for which it is to be used will be recorded.

7.7 The Police may require the relevant school to retain recordings for possible use as evidence in the future. Such records will be stored and indexed so that they can be retrieved when required.

7.8 Applications received from other outside bodies (eg, solicitors) to view or release recordings will be referred to the Headteacher. In these circumstances, recordings may be released where satisfactory evidence is produced showing that they are required for legal proceedings, an information access request (see section 8) or in response to a Court Order.

7.9 Recordings will only be released to the media for use in the investigation of a specific crime and with the written agreement of the Police.

8. SUBJECT ACCESS REQUESTS

8.1 Individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Data Protection Act 1998 and GDPR. If a request is received, individuals will be provided with the information free of charge (unless the request is manifestly unfounded or excessive, when a reasonable fee will be charged) and within one month of receipt of the request.

8.2 Recent legal cases have raised the issue of when CCTV images should be considered as personal data. Guidance arising from this implies that personal data must be substantially about the person and should affect their privacy in some way. In relation to CCTV this will not include all images:

- A wide shot of a playground or school corridor with many people in view of the cameras would not normally be considered as the personal data of all those involved. However, where a camera has picked up an individual or group of individuals specifically, or has been moved to zoom in on them, the images recorded can be considered personal data.

8.3 Where a request has been made to view an image or recording, an application must be made in writing. The individual may wish to access either a still image or part of a recording. Where third parties are included in the shots, they will be removed where this is technically possible. Where removal is not possible, their consent will be sought. Where consent is refused or where it is not possible to gain consent, a balanced decision will be made, taking conflicting interests into account, as to whether it is reasonable in all circumstances to release the information to the individual.

8.4 There is no obligation to provide information where a request has been made after CCTV records have been routinely destroyed in accordance with this policy - see 5.4 (ie, for recordings that no longer exist). However, where a request has been made for recordings still in existence, they will not be destroyed until the request is complete.

9. BREACHES OF POLICY

9.1 Any breach or alleged breach of this policy or Trust guidelines on the use of CCTV by Trust staff or other individuals will be investigated by the Headteacher.

9.2 An investigation will be carried out into any breaches of policy and procedures reviewed or put in place to ensure that the situation does not arise again.

10. COMPLAINTS

10.1 Any complaints about the operation of the CCTV system should be addressed to the Headteacher, where they will be dealt with according to the Trust's standard complaints procedures, with reference to this policy and the Trust's Data Protection policy.

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:

- the use involves the collection of new information about individuals;
- the use compels individuals to provide information about themselves;
- the information about individuals will be disclosed to organisations or people who have not previously had routine access to the information;
- we are using information about individuals for a purpose it is not currently used for, or in a way it is not currently used;
- we are using new technology that might be perceived as being privacy intrusive e.g. the use of biometrics or facial recognition; (CCTV)
- the use results in us making decisions or acting against individuals in ways that can have a significant impact on them;
- the information about individuals is of a kind particularly likely to raise privacy concerns or expectations, e.g. health records, criminal records or other information that people would consider to be private;
- the use requires us to contact individuals in ways that they may find intrusive.

Describe the service

The Castle Partnership Trust plans to use closed circuit television (CCTV) and the images produced for the purposes set out in section 3.2 of the CCTV policy.

This system includes cameras in the school's single-sex toilets, which may be considered privacy intrusive. We judge that this system in these areas is necessary and proportionate due to a previous safety incidents in school toilets where CCTV footage was able to identity the person responsible.

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 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 in the school buildings only and not at 'public space' / at wash basins not cubicles. 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	• CCTV cameras are in place throughout the site • Cameras will capture video footage and still images • No audio will be captured • All data is stored securely on a separate network and held on encrypted drives on a secure CCTV server • CCTV viewing equipment is held in a secure, locked room, access to which 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 • No live monitoring of CCTV will take place in line with our CCTV policy • CCTV footage is configured to be retained for the retention period set out in our CCTV policy and after this date it will be deleted

	Possible uses • The school will only use surveillance cameras for the purposes outlined in the CCTV policy. • Surveillance will be used as a deterrent for violent behaviour and damage to the school 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 areas. • 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

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 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 will not take place, and access to CCTV footage will be restricted as outlined in our CCTV policy. Cameras in toilets will only be able to public areas - record/monitor entrances and wash basin areas where a teacher might reasonably be present. Where video is being captured, faces can be blurred out that are not part of any incident. Cubicles and urinals are not monitored.
If a retention period is not established information might be used for longer than necessary.	Low	Breach of principle 5 of GDPR – storage limitation;	CCTV equipment configured to retain footage in line with CCTV policy (28 days). In the event of an incident that requires that footage is held for longer than this period, footage will be deleted as

		principle 2 – purpose limitation	soon as the matter is concluded.
Access to the system by unauthorised parties (Hacking)	Significant	Breach of principle 6 of 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 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 28 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. • Insurance companies to support an insurance claim.

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: A Crudgington

Date completed: 20/03/2023