



The Castle Partnership Trust

ACHIEVE | BELONG | PARTICIPATE

CCTV Use Policy

Date: March 2018

Executive Headteacher: Sarah Watson
Headteacher Court Fields School: Rachael Bennett

Lead Person: Premises Manager

1. INTRODUCTION

- 1.1 The Trust has installed a CCTV system in both 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 system comprises a number of fixed and dome cameras located around the school sites and is 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 Premises Manager in both schools 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 Premises Manager in both schools 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.

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.

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, Premises Managers and 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.

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 tapes will be referred to the Headteacher. In these circumstances, tapes 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, a fee (up to a maximum £10) can be charged and a copy of the images must be provided within 40 days of the request. When the GDPR comes into effect on 25 May 2018, 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.