

## COMDA-09-CCTV

### 1 INTRODUCTION

- 1.1 The Trust has had Closed Circuit Surveillance Cameras (also known as CCTV) for many years, both inside and outside our buildings. These were digitised around 2004-2007. The CCTV is used for the following public task duties:
- Management and security of the site,
  - Monitoring the health, safety and safeguarding of students, parents, visitors, and staff,
  - For crime prevention.
- 1.2 This policy is to ensure that CCTV within The Trust is controlled appropriately, that the data is kept secure, and to reassure those whose information is being captured, particularly given that the high-quality CCTV used by The Trust is capable of indicating “special category” data such as ethnic origin or physical disability.
- 1.3 The Trust is the Data Controller for CCTV.

### 2 ROLE OF TRUST BOARD AND COMMITTEES

- 2.1 The Trust Board has overall responsibility for ensuring compliance with all relevant data protection obligations.

### 3 ROLE OF PRINCIPAL AND SENIOR LEADERSHIP TEAM

- 3.1 The Principal acts as the representative of the Data Controller on a day-to-day basis.
- 3.2 The Data Protection Officer (DPO) is the first point of contact for individuals whose data the Trust processes, and for the Information Commissioner’s Office (ICO). The DPO is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. They will report directly to the Principal and Trust Board on any data protection issues or recommendations. The DPO role is shared with SMBC’s Information Governance Team.
- 3.3 The Principal, SLT and DPO have responsibility to authorise:
- 3.3.1 Installation, maintenance, and upgrade of the system,
- 3.3.2 Placement of the CCTV cameras:
- The data recorded should not be excessive (e.g., must not capture public areas outside of the Trust land),
  - The data recorded must not be in places where there is a reasonable expectation of privacy (e.g., toilets, changing rooms),
- 3.3.3 Placement of the CCTV monitors,
- Who has direct access to the live and recorded images,
  - Who will be permitted supervised access,

3.3.4 The following processes:

- Keeping the live and recorded images secure from non-authorized people,
- How to request supervised access to the live and recorded images and where/how to record this,
- How, and under what circumstances, images can be used, or disclosed, for example, but not limited to:
  - Disclosure to law enforcement agencies in order to assist with the prevention and/or detection of a crime,
  - Evidence of a safeguarding issue,
  - Evidence associated with disciplinary proceedings,
  - Evidence associated with complaints.

#### **4 LEGAL CONSIDERATIONS**

4.1 CCTV and the use of the images recorded on it is governed by the following acts:

- Data Protection Act (DPA) 2018,
- General Data Protection Regulations (GDPR) 2018,
- Protection of Freedoms Act (POFA) 2012,
- Freedom of Information Act (FOIA) 2000,
- Human Rights Act (HRA) 1998.

4.2 The Trust has a legal duty to comply with the relevant legislation and also with the CCTV Code of Practice (CCTVCoP) produced by the ICO and the Surveillance Camera Commissioner. This requires that:

- All authorised staffs are trained in their responsibilities under the CCTVCoP,
- aware of the restrictions in relation to access and disclosure of recorded images,
- All staffs who process data have read this policy,
- The policy is made public.

#### **5 STORING, RETENTION AND VIEWING OF LIVE AND RECORDED IMAGES**

5.1 Viewing must be kept private:

- The footage must not be overlooked,
  - Privacy screens must be used, if required,
- Discussions relating to the footage must be kept private.

5.2 Viewings *which will disclose images to a third party* must be formally requested in advance of the viewing taking place and must be requested and responded to before 14 days have elapsed. We are not allowed to charge for the provision of the data unless it is manifestly unfounded or excessive. The request must be handled via the DPO.

5.2.1 The request must be in writing and must contain the following details:

- Purpose of and/or reason for the search,
- Requesting person,
- Approximate start/end date and time of the event,
- Location(s) of the event,
- Relationship/responsibility to person/people in the recording:
  - If there is no relationship to the people in the footage this must be carefully managed to ensure that a Data Breach does not occur,
- If it is a law-enforcement request the following protocols must be presented to the DPO:
  - Be provided in writing, using the appropriate form (currently WA170),
  - Signed by authorising officer,
  - Refer to the name and section of the legislation which entitles them to receive the information.
- See the Procedure COMDA-P09-1-CCTV-Request to View-00

5.2.2 The outcome of the search must also be recorded by the DPO:

- The outcome of the viewing/search (successful or not),
- Who was present during the viewing,
- Actual start/end date and time of the event,
- Start date, time, and duration of review,
- Any other information.

5.3 Use with Behaviour and Complaints procedures:

5.3.1 This data may be used within the Trust's discipline and complaints procedures, as required,

5.3.2 This is subject to the usual confidentiality requirements of those procedures.

5.4 Routine footage must be kept for a maximum of 40 calendar days:

- This is controlled by the CCTV system:
  - The data is stored on local servers,
    - These are kept in a secured room,
    - They are accessible only via password-controlled systems.
  - The cameras are motion-triggered; each has its own storage area on the server,
  - Some areas of the school are busier than others. Different places in the school, different times and different days will give different volumes of data and hence will be retained for different lengths of time,
  - The data may be overwritten within 14-21 days but may last 30-40.

5.5 Incident footage under investigation must be downloaded in advance of deletion:

- The quality of the images must be maintained,
- A *copy* of the stored footage must be edited to obscure e.g., faces, identifying features if it needs to be disclosed to e.g., parents, so that a data breach does not occur,
- If the data is to remain on the school site it must be kept in a secure area, which is only accessible to authorised personnel,
- If the data is being transferred off-site it must be stored on an encrypted device or transferred online in encrypted format,
  - The encryption password must be kept separately, and securely, from the encrypted data,
  - The encryption password must be transferred separately from the encrypted data.
- When the action/investigation of the footage is complete, it, and all copies of it, must be permanently and securely deleted.

## 6 CRIMINAL OFFENCES RECORDED ON CCTV

6.1 Where a potential or alleged criminal or civil offence has taken place on The Trust's premises and has been recorded on the CCTV the data cannot be released to any party other than the police. There is no duty to release the footage to:

- The subject,
- Their family,
- Their friends.

6.2 The footage of the incident must be immediately downloaded to a secure area, waiting for a valid police request, at which point the data should be securely transferred.

6.3 Any request received which is part of an ongoing police investigation will be denied. The record of any viewing(s) which have taken prior to the raising of the police investigation will be passed onto the police, along with the footage and may have an impact on the process of the police investigation.

## 7 SIGNAGE

7.1 Signage must be prominently displayed at entrances to the Trust's CCTV area to ensure that all people on site are clearly informed that:

- CCTV footage is being recorded,
- Who to contact should they wish to make an enquiry.

## 8 AUTHORISATION OF STAFF, SPECIAL CIRCUMSTANCES

8.1 Contractors who need to view the recordings must follow the same request procedure as outlined in 5.2. This clause excludes e.g., maintenance and enhancement of the system, which should, if possible, be completed during vacation, periods of closure.

8.2 If a lawful organisation makes a request for Covert monitoring, it must be requested with evidence of a Record of Information Processing (RIPA) request and passed onto the DPO for scrutiny. More information may be requested, as necessary to justify the request.

## 9 MISCONDUCT

9.1 Non-compliance with this policy constitutes misconduct and is a disciplinary offence.

Where misconduct is known the disciplinary procedure will apply.

**10 AUTHOR**

10.1 The author of this policy is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

**11 VERSION CONTROL**

<b>Policy Number</b>	COMDA-09
<b>Policy Name</b>	CCTV
<b>Version Number</b>	03
<b>Publication Method</b>	External  A copy must be made available in U:\Staff Information\Policies\COMMunications and DAta Policies
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	May 2023
<b>Key changes since previous version</b>	1. Clarify the situation with regard to ongoing investigations, following guidance from West Midlands Police.
<b>Next review date</b>	February 2024

## PROCEDURE

### **COMDA-P09-1-CCTV-REQUEST TO VIEW**

#### **1 INTRODUCTION**

- 1.1 Viewings of CCTV can only be viewed by authorised people unless a formal request has been received and agreed
- 1.2 This procedure explains how to make a formal request

#### **2 TASK DESCRIPTION**

- 2.1 All requests for non-authorised people to view CCTV footage must be made in writing.
- 2.2 The request will be reviewed by the Data Protection Officer, or a Pastoral Manager. All requests which are part of a police investigation are automatically refused.
- 2.3 You will be informed of the conclusion of the review.
- 2.4 If the request is justified:
  - A suitable date/time/place will be arranged for the viewing,
  - The outcome of the viewing/search will be recorded,
  - The actual start/end date/time of the event will be recorded,
  - The start/end date and time of the viewing will be recorded,
  - Any other information relating to the viewing will be recorded.

#### **3 PROCEDURAL DETAILS**

- 3.1 Staff: go to Microsoft Form <https://forms.office.com/r/myvXncSpAn>, and complete it if you want to see footage in person. Of preference, ask one of the authorised CCTV staff to view the footage for you.
- 3.2 For parents, or external organisations: use the form COMDA-09-CCTV-Request-to View. Complete it and send a photograph or scan of it to [dataprotection@heart-england.co.uk](mailto:dataprotection@heart-england.co.uk).
- 3.3 Records relating to viewings will be stored in U:\Staff Information\Data Protection\CCTV viewings.



**PROCEDURE**

**4 PROCEDURE AUTHOR**

- 4.1 The author of this procedure is the Data Protection Officer. They should be contacted for any points of clarification or suggested future amendments.

**5 VERSION CONTROL**

<b>Procedure Number</b>	COMDA-P09-1
<b>Procedure Name</b>	CCTV-Request to view
<b>Version Number</b>	02
<b>Publication Method</b>	External  A copy must be kept in U:\Staff Information\Policies\Procedures for Policies\COMmunications and DAta Procedures
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	May 2023
<b>Key changes since previous version</b>	1. Addition of "All requests which are part of a police investigation are automatically refused." to point 2.2
<b>Next Review Date</b>	February 2024



**APPENDIX**

**COMDA-A09-1-CCTV-REQUEST TO VIEW**

**1 INTRODUCTION**

- 1.1 The form **on the next page** is the one you must complete when you want to look at CCTV that has been recorded in school.
- 1.2 This is linked to the CCTV policy and Appendix

**2 APPENDIX AUTHOR**

- 2.1 The author of this appendix is the Compliance Officer. They should be contacted for any points of clarification or suggested future amendments.

**3 VERSION CONTROL**

<b>Appendix Number</b>	COMDA-A09-1
<b>Appendix Name</b>	CCTV – Request to View
<b>Version Number</b>	00
External	External  A copy must be made available in U:\Staff Information\Policies\Appendices for Policies\ COMMUNICATIONS and DATA Appendices
<b>Approved by</b>	Full Trust Board
<b>Date of Approval</b>	May 2023
<b>Key changes since previous version</b>	1. Aid Clarity
<b>Next Review Date</b>	February 2024





**APPENDIX**

**PARENTS/EXTERNAL REQUEST FOR CCTV VIEWING**

Please complete this form and then send a scan/photograph of it to  
DataProtection@heart-england.co.uk

Your Name		
Your email address		
Your phone number		

Please explain below why you want to see the recorded CCTV footage:

What Day and Date did the incident take place?	Roughly what time did the incident take place?	Location of the incident.	
Relationship to the student involved			
Your signature		Date	
Is this a law-enforcement request	Yes – Form WA170 will be required		
	No		

If the CCTV footage is part of a police investigation your request-to-see has to be denied.  
All records of viewings are sent to the police when they request video footage.