CCTV Policy

Version: 1.3

Important: This document can only be considered valid when viewed on the Trust website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Stephen Dale, Project Director
Name of Responsible Committee/Individual:	Trust Board
Implementation Date:	26 February 2018
Review Date:	26 February 2021
Target Audience:	All staff, students and visitors

CONTENTS

Glossary

ACoP	Approved Code of Practice
BS	British Standard
DfE	Department for Education
H&S	Health and Safety
HSE	Health & Safety Executive
HSG	Health & Safety Guidance
IT	Information Technology
UK	United Kingdom

CHANGE RECORD

Version	Date	Change details
1.1	14 September 2017	Initial draft
1.2	11 January 2018	Change to charging section
1.3	26 February 2018	Addition of GDPR section and amendements to the Subject Access Request sections,

1. INTRODUCTION

This policy covers the requirements detailed in the Data Protection Act 1998, Human Rights Act 1998, CCTV Code of Practice 2008 and Protection of Freedom Act 2012 and is aimed at the use of CCTV and similar surveillance equipment that monitors and records images from applicable areas.

The primary objectives being:

- Prevention and detection of crime
- Public safety
- Maintenance of the public perception of the Education Alliance

2. SCOPE

This policy sets out The Education Alliance's approach to the management of Close Circuit Television (CCTV) throughout the organisation and applies to all directly and indirectly employed staff and other persons working within the organisation. The policy has particular relevance for those staff members who have responsibility for using or managing CCTV systems or acting as The Education Alliance's point of contact for enquiries.

3. POLICY STATEMENT

The Education Alliance is committed to ensuring compliance with legal requirements using them as a minimum standards and seeking to exceed those standards in order to protect students, staff and visitors.

The Education Alliance aims to balance the rights and responsibilities of people using its services with those of employees, with a clear approach to Security Management.

The intended outcome of this policy is to provide the organisation and its staff with the knowledge and skills to effectively reduce and manage the risk from adverse risks in the workplace.

The objectives are to:

- Ensure a safe and secure working environment for students, staff and visitors.
- Identify who is responsible for CCTV systems within the organisation and the remit and scope of their roles.
- Ensure The Education Alliance's employees are aware of, and can access mechanisms to maintain and improve working environments.
- Prevent unfair intrusion into the privacy of members of the public and students.

4. DUTIES AND RESPONSIBILITIES

4.1 Board of Trustees

The Board of Trustees has overall responsibility for monitoring compliance with and effectiveness of all The Education Alliance policies and will ensure that effective management systems are in place to achieve high standards of health, safety and welfare.

4.2 Chief Executive Officer

The Chief Executive Officer is the Accountable Officer and has overall responsibility for health, safety and security matters and will ensure that this policy is implemented in all directorates and reviewed on a regular basis.

4.3 Heads of School

The Head of School has lead responsibility for Security Management and delegates day to day management to the Premises Manager at each site.

The Head of School and General Data Protection Regulation (GDPR) Officer, supported by the assigned lead(s) for each school (see Section 4.5), must be consulted regarding operational requirements, appropriateness and need for new or replacement CCTV systems and must hold a comprehensive list of CCTV cameras across the organisation.

4.4 Premises Managers

Premises Managers are responsible for:

- Day to day security of their working areas and implementation of The Education Alliance's security procedures
- Ensuring all staff report breaches of security, criminal activity, incidents, CCTV systems failure, or suspicions in the area where they work immediately
- Ensuring that systems and procedures are in place on the site for which they have responsibility to ensure compliance with this policy and the Information Commissioner's Code of Practice

4.5 General Data Protection Regulation (GDPR) Officer

The GDPR Officer is responsible for:

- Receiving, assessing and processing Subject Access Requests
- Carrying out Subject Access Requests
  Note: In addition to The Education Alliance's GDPR, a minimum of two further people within each secondary school (primary schools will be overseen by their HUB secondary school) to be

trained and nominated to carry out Subject Access Requests and operate CCTV equipment on behalf of their nominated school(s)
- Providing advice on the provision of access and material to law enforcement agencies including the Police, as well as advising on the provisions of the CCTV Codes of Practice.
- Ensuring that this policy allows The Education Alliance to comply with their legal responsibilities.

4.6 ICT Managers

ICT Managers are responsible for:

- Ensuring the CCTV systems within their area of responsibility are functioning correctly

4.7 Employees

Employees have a responsibility to abide by this policy and any decisions arising from the implementation of it.

Employees also have responsibility for:

- Taking effective measures to ensure The Education Alliance's premises and property is maintained in a secure condition
- Taking steps to safeguard against loss of The Education Alliance's property and the property of individuals
- Taking reasonable steps to ensure security of their own personal possessions – the Education Alliance takes no responsibility for personal possessions except in specific circumstances

5. PROCEDURES

5.1 Purpose of CCTV Use within The Education Alliance

Within The Education Alliance CCTV is used for the following purposes:

- The prevention and detection of crime - National Security
- The prosecution of offenders
- The management of safety and security for students under The Education Alliance's Child Protection Policies
- The management of safety and security for staff, visitors and the public
- Should there be any alleged breaches of Education Alliance rules, the CCTV may be used in disciplinary action
- Investigate allegations or serious concerns about possible crime

5.2 Siting of Cameras

It is essential that the location of the equipment is carefully considered, because the way in which images are captured must comply with the following standards:

- The equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment and this must not include toilets or changing rooms
- If residential areas are not intended to be covered by the CCTV system and they border The Education Alliance's grounds, then The Education Alliance should consult with the resident if images might be recorded
- Operators must be aware of the purpose(s) for which the scheme has been established
- Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed
- If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces which are not intended to be covered by the scheme
- If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered
- Where practicable, systems should be capable of masking neighbouring spaces to prevent inadvertent collateral intrusion
- The equipment is not to be placed where privacy and dignity of a student may be compromised. This includes toilet areas, changing rooms or similar

5.3 Camera Signs

Signs must be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The size of signs will vary according to circumstances. The signs must be clearly visible and legible and contain the following information:

- Identity of the person or organisation responsible for the scheme
- The purposes of the scheme
- Details of whom to contact regarding the scheme i.e. the telephone number of reception/control room where the equipment is used.

5.4 Quality of Images

Images produced by the equipment must be of sufficient quality as to enable the identification of persons suspected of committing criminal acts, witnessing such acts or in support of other security issues from recorded images.

The CCTV system should be regularly checked to ensure that the recorded images are of good quality, the date and time of the system checked for accuracy, a check that the cameras are working and the quality of the recorded image is sufficient. .

Any problems should be rectified as soon as is practicable by requesting assistance through the Estates Department.

5.5 Storage and Retention of Images

Storage and Retention of images:

- Shall only be used for the purpose defined in this policy
- Shall not be sold or used for commercial purposes or the provision of entertainment
- Remain the property of The Education Alliance
- Should not be retained for longer than necessary
- Once this period has expired then the images should be confidentially erased
- Images are digitally recorded and stored securely within the system's hard drives for up to 30 days when they are then automatically erased as part of an on-going rolling programme
- Where the images are required for evidential purposes in legal or Trust disciplinary proceedings, they can either be stored in a secure password protected area of the hard drive in separate file or downloaded onto cd-r

5.6 Viewing of Images by Staff (Live and Recorded)

CCTV images can only be viewed when necessary. This information is only to be accessed by authorised staff, who as detailed in section 4.5 will be The Education Alliance's GDPR **i**n addition to a further two nominated individuals within each secondary school who have been suitably trained and licensed. All other staff, students and visitors must be clear of this area and the area closed.

Recorded images should be viewed in a restricted area, such as a designated secure office.

The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to fully authorised persons only.

Any viewing of images should be documented on the Viewing of CCTV Images Form (Appendix 1) and sent to the GDPR.

5.7 Subject Access Requests

An individual may request a copy of any recording that exists of them. The GDPR has responsibility for the receiving and logging all Subject Access Requests and should deal with all requests. All staff involved in operating the equipment must be able to recognise a request for access. Individuals requesting access (the Data Subjects) should be provided with:

- A Request for CCTV Image – Subject Access under Data Protection Act 1998 form which indicates the information required to locate the images requested. (Appendix 2)
- This policy, which describes the types of images which are recorded and what purpose they are recorded for

Access may be denied where such an action would compromise the detection or prevention of crime, or where it may impede the apprehension or prosecution of offenders.

5.8 Disclosure, Viewing & the Provision of Copies of Images by the Data Subject

If the individual making the request is unknown to The Education Alliance, a photograph of the individual may be requested in order to locate the correct image. A written response should be sent to the individual within 21 days of receipt of the request, confirming whether images are held and including details for arranging a viewing, if appropriate. It is a requirement of the Data Protection Act to provide the information (or refusal notice) to the individual within 30 days of their original request.

The GDPR should determine whether disclosure to the individual would entail disclosing third party images. If third party images are to be disclosed as an incidental part of the recording, then the GDPR or other trained individual should arrange for the images of third parties to be disguised, blurred, redacted or obscured.

5.8.1 Disclosure, Viewing and the Provision of Copies of Images by Third Parties – Police, Insurance companies (i.e. not the data subject)

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, to ensure that the rights of individuals are preserved.

Disclosure of the recorded images, whether motion or still images, to third parties should only be made in limited circumstances. Reason(s) for which they may disclose copies of the images are compatible with the registered reason(s) or purpose(s) for which they originally obtained those images.

All requests for images must be made in writing to the GDPR. The Request for CCTV Image – Subject Access Request form (Appendix 2) should be provided by the requestor along with any required fee (maximum £10) prior to the release of any images or video footage.

All access by 3rd parties to the device on which the images are recorded should be documented on the Viewing of CCTV Images Form (Appendix 1).

Access to the data will be given to the Police subject to the requirements of any Information Sharing Agreement. Access should be recorded on the form for 'Application for access to CCTV images by the Authorised Agency (Police)' (Appendix 3). Two copies of the images will be made showing the incident(s), one for the third party and one to be retained securely either on site or with the GDPR.

5.8.2 Disclosure of CCTV Footage to the Media

If images are to be disclosed to the media, the images of individuals not involved in the incident in question will need to be disguised or blurred so that they are not readily identifiable. If the system does not have this type of facility then an editing company will need to be contracted to perform this function.

The decision to release CCTV footage to the media in non-police cases can only be taken by the Chief Executive Officer and GDPR.

5.9 Documentation

All documentation relating to the management and operation of CCTV together with all Subject Access Request forms must be securely retained for a minimum of 3 years, followed by confidentially destroying. Any images that have been retained for evidential purposes will be retained for the minimum period necessary to serve that

purpose which will necessarily need to be decided on a case by case basis.

5.10 Use of CCTV Footage for Disciplinary Purposes

Only in the circumstances detailed in this section may CCTV footage be used in proceedings under Disciplinary Policy i.e. a criminal activity.

In the event that recorded CCTV footage reveals activity that The Education Alliance could not reasonably be expected to ignore i.e. criminal activity, then the relevant CCTV footage may be considered during investigatory stages of the formal disciplinary process, and later used in formal disciplinary hearings, if relevant to the allegations against the employee.

If such CCTV footage is identified it will be presented to the employee in the usual way, pursuant to the Disciplinary Policy. Wherever possible, the employee will be given the opportunity to review the CCTV footage and explain or challenge its content. The employee will also be permitted to make representations with regard to the CCTV footage in any disciplinary hearing.

6.0 Training

All personnel who are required to operate or manage a CCTV system are to be properly trained and appropriately licensed i.e. hold a valid Security Industry Authority (SIA) licence. These individuals must also be competent in producing evidential material from the system for which they are responsible.

The provision of training for non-security personnel should be written in to the installation contracts for all future, new and refurbished systems to ensure compliance. Local staff must be trained to conduct routine systems checks in accordance with this policy; including date/time stamp corrections. They should also be trained to produce evidential image discs for the police.

7.0 References/Evidence/Glossary/Definitions

The following items of legislation are relevant to this policy:

- Crime and Disorder Act 1998
- Criminal Justice and Public Order Act 1994
- Criminal Procedure and Investigations Act 1996
- Data Protection Act 1998
- Human Rights Act 1998
- Private Security Industry Act 2001
- Police and Criminal Evidence Act 1984
- Protection of Freedom Act 2012

- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000

The following External publications have helped inform the development of this policy:

- CCTV Code of Practice 2008, Information Commissioner's Office, January 2008
- CCTV Operational Requirements Manual - Is your CCTV system fit for purpose? N Cohen, J Gattuso, K MacLennan-Brown, 2009

The following internal documents have also been considered when developing this policy:

- The Information commissioner's Code of Practice on CCTV systems available on the web at http://www.dataprotection.gov.uk under 'Guidance and other Publications' and then 'Codes of Practice our responses and other papers'
- The Information Commissioner's publication 'The Data Protection Act 1998: Legal Guidance' available on the web at http://www.dataprotection.gov.uk under 'Guidance and other Publications' and then 'Legal guidance'
- British Standards Institute publications BS 7958:1991 'Closed Circuit Television (CCTV) – Management and Operation Code of Practice'
- UK Police Requirements for Digital CCTV Systems.
- CCTV Operational Requirements Manual, Publication No. 55/06, Home Office Scientific Development Branch.

Appendix 1 - Request by Third Party or Education Alliance Staff to View CCTV Images Form

The date and time of viewing	
The name of the operator removing the images for viewing	
The name of the person(s) viewing the images (If this includes third parties, then the name of the person and the organisation should be included).	
The reason for the removal, where the CDR/DVDR is removed.	
The outcome, if any, of the viewing.	

Please send completed forms to:

General Data Protection Regulation Officer
The Education Alliance c/o Malet Lambert
James Reckitt Avenue
Kingston-Upon-Hull
HU8 0JD

Appendix 2 - Request for CCTV Image/Disk

NOTES TO ASSIST IN COMPLETION OF THE FORM

DECLARATION (Note 2)

The person making the application must complete this section.

a) If you are the data subject – tick the first box and sign the authorisation then proceed to section 5.

b) If you are completing this application on behalf of another person, in most instances, we will require their authorisation before we can release the data to you. The data subject whose information is being requested should be asked to complete the 'Authorisation' section of the form. (Section 5)

c) If the data subject is a child i.e. under 16 years of age the application may be made by someone with parental responsibilities, in most cases this means a parent or guardian. If the child is capable of understanding the nature of the application his/her consent should be obtained or alternatively the child may submit an application on their own behalf. Generally children will be presumed to understand the nature of the application if aged between 12 and 16. However, all cases will be considered individually.

REQUEST FOR CCTV IMAGE/DISK
SUBJECT ACCESS UNDER DATA PROTECTION ACT 1998

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.

SECTION 1: DATA SUBJECT DETAILS

Please supply a photo to aid in identification:

PHOTO

SURNAME:	**DATE OF BIRTH:**
FORENAME(S):	**SEX:**
Address: **Postcode:**	**Home Telephone No:** **Work Telephone No:**

Proof of identity

To help establish your identity, your application must be accompanied by TWO official documents that, between them prove your identity and address

Current signed passport	Proof of address
Residence permit issued by the Home office	Recent (within 3 months) utility bill
Current UK photo card driving licence	Local authority council tax bill
Birth certificate	Current UK photo care licence
HM Forces ID Card	Bank, building society passbook
Adoption Certificate	Current local council rent book
Marriage/civil partnership certificate	Department of Works and Pensions original notification letter
Divorce or annulment papers	Court Order (within 12 months of current date)

SECTION 2: DECLARATION STATEMENT (Note 2)

This section must be signed in the presence of the person who certifies your application.

I declare that the information in this form is correct to the best of my knowledge and that I am entitled to apply for access to personal data referred under the terms of the Data Protection Act 1998.

Please tick appropriate box

I am the person named Signature of Data Subject: Date: **or**	
I am the agent for the person named and I have completed the authorisation section	
I am the parent/guardian of the person who is under 16 years old and has completed the authorisation section	
I have been appointed by the Court to manage the affairs of the person	

SECTION 3: APPLICANT DETAILS - The applicant is the person who is applying on behalf of the data subject to get access to the CCTV footage.

Applicants Name (please print)	
Address to which reply should be sent (if different from over, inc Postcode)	
Signature of Applicant	

SECTION 4: LOCATION - Provide details of the camera location, and the date and time of the footage you would like to see, as well as a general description of the incident

To help us find the information

Date and time of incident	
Place incident occurred	

Brief description of incident	

SECTION 5: AUTHORISATION STATEMENT

I hereby authorise The Education Alliance to release CCTV images they may hold relating to me to …… (enter the name of the person acting on your behalf) to whom I have give consent to act on my behalf.

Signature of Data Subject **Date ……**

OFFICIAL USE ONLY

Date Request Received		Amount Paid	
Date Form sent to Applicant		Method of Payment	
Date Form Returned		Date sent to System Administrator	
Certification Checked		Data checked	
		Date completed	

Please send completed forms to:

General Data Protection Regulation Officer
The Education Alliance c/o Malet Lambert
James Reckitt Avenue
Kingston-Upon-Hull
HU8 0JD

Appendix 3 - Application for Access to CCTV Images by Authorised Agency (Police)

1. Applying Agency:
2. Person applying:
3. Position:
4. Reason for request:
5. Reason and appropriateness of application:
6. Date:

Authorisation:

Authorised by:
Position:
Date:

OFFICIAL USE ONLY

Date Request Received		Amount Paid	
Date Form sent to Applicant		Method of Payment	
Date Form Returned		Date sent to System Administrator	
Certification Checked		Data checked	
		Date completed	

Please send completed forms to:

General Data Protection Regulation Officer
The Education Alliance c/o Malet Lambert
James Reckitt Avenue
Kingston-Upon-Hull
HU8 0JD