Closed Circuit Television (CCTV) Policy

Document provenance

This policy was approved as follows	
The Executive Leadership Team	Date: [date approved]
Frequency of review: Annually	
ELT Owner: Chris Wiseman, Deputy CEO/Chief Operating Officer	

Summary of changes at last review:

- None - New policy implemented for 01 September 2019

Related documents:

- Subject Access Request Guidance
- Data Breach Policy
- Information and Records Retention Policy
- Information Security Policy
- Privacy Notices
- Procedure for Police and other Organisation Requests for Information under Schedule 2 Part 1 Para. 2 Data Protection Act 2018 (*Previously a request under Section 29 of the Data Protection Act 1998)*

CCTV Policy

1. Policy Statement

1.1. This document sets out the appropriate actions and procedures, which must be followed to comply with data protection legislation in respect of the use of CCTV (closed circuit television) surveillance systems managed by E-ACT.

1.2. We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our staff, pupils and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns.

1.3. Images recorded by surveillance systems are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, pupils and visitors, relating to their personal data, are recognised and respected.

1.4. This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

2. Scope

2.1. This policy applies to all E-ACT buildings and estates.

3. CCTV usage

3.1. We currently use CCTV cameras to view and record individuals on and around our premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice.

3.2. We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

3.3. This policy covers all employees, contractors, trustees, volunteers and any other individuals engaged to perform services for E-ACT. This policy is available on the academy website and a hard copy can be obtained from the academy office. This policy has been reviewed by the Trust Data Protection Officer (DPO) and approved by the Executive Leadership Team (ELT). The Trust's privacy notices for staff, parents and pupils include information about the use of

CCTV by the Trust including for what purpose it is used. A copy of the privacy notices can be found here.

3.4. Authorised Employees with their permitted activities are defined in the table below:

Table 1

Viewing and Downloading Function:		
1	Regional Operations Directors	
2	Regional Facilities Managers	
3	Senior Site Team	*only with the express permission of 1 or 2 above*
4	IT Support	
Viewing Only Function:		
5	Headteachers	
6	Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL) in the academy Regional Safeguarding System Leader (RSSL)	
7	Other Staff Members (*for positive identification of individuals*)	*only with the express permission of 1, 2 or 5 above*

Breaches of this policy

3.5. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

3.6. Any information security breach (for example, unauthorised access to CCTV footage) must be reported immediately to the DPO in accordance with the Trust's Data Breach Policy.

3.7. All authorised employees viewing CCTV images are responsible for each viewing of the images, which must be justifiable. All authorised employees viewing CCTV images must be aware of their obligations under the data protection legislation when viewing images. If you are in any doubt as to what those obligations are, please speak with the DPO.

4. Responsibilities

4.1. The Board of Trustees has overall accountability and responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the Chief Operating Officer (COO). Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Regional Operations Director (ROD).

4.2. This policy will be maintained and reviewed at least annually under the supervision of the Trust DPO to ensure that the use of CCTV continues to be justified and that the appropriate measures are in place to mitigate data protection risks raised by its use.

5. Purpose of the CCTV System

5.1. We currently use CCTV on our premises for the following reasons:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of pupils, staff, visitors and other members of the public and to act as a deterrent against crime;
- to support law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist in the day-to-day management, including ensuring the health and safety of pupils, staff and others; and
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.

5.2. This list is not exhaustive and other purposes may be or become relevant.

6. Monitoring

6.1. Cameras are situated to ensure they cover Trust premises as far as is possible, including the exterior of buildings, vulnerable public facing areas, car parks, outside spaces, communal areas within buildings and both the main entrance and secondary exits.

6.2. The CCTV system is currently in operation and capable of being monitored 24 hours a day, every day of the year.

6.3. As far as practically possible CCTV cameras will not focus on private homes, gardens or other areas of private property.

6.4. Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a Data Privacy Impact Assessment (DPIA).

6.5. Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

7. How will we operate any CCTV?

7.1. We will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of which

organisation is monitoring the CCTV (if not wholly operated by E-ACT) and who to contact for further information, where these things are not obvious to those being monitored.

7.2. We will ensure that live feeds from cameras and recorded images are only viewed by Authorised Employees whose role requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

7.3. We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or equivalent serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

7.4. In the unlikely event that covert monitoring is considered to be justified, the School will carry out a Data Protection Impact Assessment (please see section 6.4 above for more information). The rights of individuals whose images may be captured will always be taken into account in reaching any such decision.

8. Use of data gathered by CCTV

8.1. In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so, as detailed in E-ACT's Information Security Policy.

8.2. We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data where this is the case.

8.3. CCTV images may only be viewed by Authorised Employees. All Authorised Employees viewing the CCTV images will act with utmost probity at all times. All images viewed by Authorised Employees must be treated as confidential.

8.4. All Authorised Employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.

8.5. All Authorised Employees viewing CCTV images are responsible for their every viewing of the images, which must be justifiable.

9. Retention and erasure of data gathered by CCTV

9.1. Data recorded by the CCTV system will be stored securely and digitally on the servers for the academy. Data from CCTV cameras will not be retained indefinitely and in any case deleted after 30 days' maximum from the date the recording is made, if not subject to an ongoing incident being investigated or a legitimate access request from a data subject.

9.2. At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

9.3. Routine checks are made to ensure that the system is operating in accordance with the terms of this policy and that information relating to the recordings (date, time etc.) are accurate; these details are entered into the CCTV Download and Maintenance Log Book (the Log Book – see Appendix 2).

10. Use of additional surveillance systems

10.1. A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

10.2. No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in toilets and changing rooms).

11. Requests for access and disclosure

11.1. Access will only ever be permitted to Authorised Employees for the purposes of performing their function within E-ACT. Downloading images is strictly controlled and limited as set out in 3.4.

11.2. Procedures for managing the saved data is detailed in the Log Book (Appendix 2) – staff are trained to understand the administrative regime to control the use of the images.

11.3. Access to images by academy staff is strictly controlled and limited as set out in 3.4.

11.4. No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Regional Operations Director. Any recordings which are shared with third parties will be encrypted unless there is a good reason for not doing so. This reason will be recorded in the Log Book (Appendix 2). Data will not normally be released unless satisfactory evidence that it is required in connection with legal proceedings or if a court order has been produced.

11.5. In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime. Only written requests made under Schedule 2 Part 1 Para. 2 Data Protection Act 2018 (previously Section 29 Request) will be considered (see Appendix 1 for Request form). Such requests must specify the date and time (as far as possible) of the images required. If CCTV footage is disclosed to a law enforcement agency the Trust will record what information has been disclosed, when the disclosure was made, to whom it was disclosed and for what purpose(s)

in the Log Book (Appendix 2). If the decision is taken not to release the images, then the image in question will be held and not destroyed until all legal avenues have been exhausted.

11.6. We will maintain a record of all disclosures of CCTV footage.

11.7. No images from CCTV should ever be posted online or disclosed to the media by any member of staff.

12. Internal use of CCTV

12.1. If a member of staff considers that CCTV footage might be needed for an internal matter (e.g. a pupil disciplinary issue) they should speak to the Regional Operations Director in the first instance.

13.Data Subject access requests (DSARs)

13.1. Data subjects may make a request for disclosure of their personal information (known as a data subject access request or subject access requests) and this may include CCTV images. How the Trust deals with subject access requests more generally is set out in the Subject Access Request Guidance.

13.2. In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

13.3. We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

14. Legal basis for processing

14.1. Under data protection law the Trust must set out the bases it is relying on to make and use CCTV footage.

14.2. The Trust considers that the following bases are applicable:

14.2.1. The Trust has a legitimate interest in using CCTV for the purposes described at paragraph 4 above. In addition, others, such as pupils, parents, and visitors to the School site, also have a legitimate interest in the School's use of CCTV (e.g. so that they are confident that the Trust sites are safe).

14.2.2. The use of CCTV is not unfair because the Trust has put measures in place to safeguard the rights of individuals identifiable from CCTV, as described in this policy.

14.2.3. The use of CCTV for the purposes described in paragraph 4 is also in the public interest.

14.3. Sometimes the Trust's use of CCTV will be necessary for compliance with a legal obligation for example, where it is required to disclose CCTV footage to the Police in accordance with a court order.

15.Complaints

15.1. If any member of staff has questions about this Policy or any concerns about our use of CCTV, they should speak to their line manager or headteacher in the first instance.

15.2. Where this is not appropriate or matters cannot be resolved informally, employees should use our formal Grievance Policy and Procedure.

16.Requests to prevent processing

16.1. We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact our Data Protection Officer DPO@E-ACT.org.uk.

Appendix 1

Request for Disclosure of Personal Data under Schedule 2 Part 1 Para. 2 Data Protection Act 2018

(Previously Section 29 Request)

(For guidance on completing this form, please see Procedure for Police and other Organisation Requests document)

1. Requestor

First name(s):		**Last name:**	
Job title *(rank)*:		**Collar No:**	
Organisation:			
Address:			
Postcode:		**Telephone:**	
Email:			

2. Data subject

Current details

First name(s):		**Last name:**	
Address:			

Other identifying information *(including details of any additional documents attached)*:

Specific information required

3. Reason for requesting disclosure

Offence(s)

☐ Unable to specify offence due to risk of prejudicing the case

Statutory powers *(Do not cite Schedule 2 Part 1 Para. 2 Data Protection Act 2018)*

Purpose

State the purpose for requesting disclosure of personal information about the data subject specified in section 2 of this form. Select one option

☐ Prevention or detection of crime

☐ Apprehension or prosecution of offenders

☐ Assessment or collection of tax, statutory duty or imposition of a similar nature

☐ Protecting the vital interests of a person

How would not providing the information requested prejudice the stated purpose?

4. Information provision

If we hold information how would you like the information to be provided?

☐ Electronically via secure email

☐ Collection in person (Proof of identification required when collecting)

We will notify you if we do not hold information or your request for disclosure is refused

Date Information required: *(it may take up to 5 working days to process)*	

5. Declaration and authorisation

The authorising officer must be of the rank of police inspector or higher, or for other 'relevant bodies' a senior officer/manger. In the case of an inspector not being available at your location, we will accept an email from an inspector (or higher ranking officer) attaching this paperwork and confirming their approval.

Declaration

I certify that:

- Information requested is compatible with the stated purpose (section 4) and will not be used in anyway incompatible with that purpose
- I understand information given on this form is correct
- I understand that if any information given on this form is incorrect, I may be committing an offence under Section 170 Data Protection Act 2018

Requestor

Signed:		**Date:**	

Authorising Officer

First name:		**Last name:**	
Job title:			
Signed:		**Date:**	

Where to send your request

Please note: If the form has not been fully or properly completed and authorised you will be asked to re-submit your application. Please hand this form to a member of academy office staff to be submitted to the Data Protection Officer, or send this form to:

Email: DPO@E-ACT.org.uk

Postal address: Data Protection Officer, E-ACT, Innovation Centre, Primley Avenue**,** Walsall**,** West Midlands WS2 9UA

Appendix 2

CCTV DOWNLOAD AND MAINTENANCE LOG BOOK

Academy: _____

Building Name: _____ **CCTV Log Page Number:** _____ *(Ensure sequential numbering)*

Date and Time:	**Staff Name:**	**Camera Details (*Location and Number*):**	**Reason for Viewing/Downloading**	**If viewing/ downloading for Police confirm receipt of written Request**	**If Incident, give brief description of incident and action taken:**	**If Fault, give details of fault/maintenance and action taken:**

Explanatory notes (i) Viewing of recorded images should take place in a secure, restricted area (ii) Only Authorised Employees are permitted to view recorded images (iii) The Regional Operations Director should be informed in all cases where an incident is reported to the police (iv) Log books must be sequential in order so that pages or entries cannot be removed and full and accurate records are kept.

Appendix 1

Request for Disclosure of Personal Data under Schedule 2 Part 1 Para. 2 Data Protection Act 2018

(Previously Section 29 Request)

(For guidance on completing this form, please see Procedure for Police and other Organisation Requests document)

1. Requestor

First name(s):		**Last name:**	
Job title *(rank)*:		**Collar No:**	
Organisation:			
Address:			
Postcode:		**Telephone:**	
Email:			

2. Data subject

Current details

First name(s):		**Last name:**	
Address:			

Other identifying information:

Specific information required

3. Reason for requesting disclosure

Offence(s)

☐ Unable to specify offence due to risk of prejudicing the case

Statutory powers *(Do not cite Schedule 2 Part 1 Para. 2 Data Protection Act 2018)*

Purpose

State the purpose for requesting disclosure of personal information about the data subject specified in section 2 of this form. Select one option

☐ Prevention or detection of crime

☐ Apprehension or prosecution of offenders

☐ Assessment or collection of tax, statutory duty or imposition of a similar nature

☐ Protecting the vital interests of a person

How would not providing the information requested prejudice the stated purpose?

4. Information provision

If we hold information how would you like the information to be provided?

☐ Electronically via secure (password protected) email

☐ Collection in person (Proof of identification required when collecting)

We will notify you if we do not hold information or your request for disclosure is refused.

Date Information required: *(it may take up to 5 working days to process)*	

5. Declaration and authorisation

The authorising officer must be of the rank of police inspector or higher, or for other 'relevant bodies' a senior officer/manger. In the case of an inspector not being available at your location, we will accept an email from an inspector (or higher ranking officer) attaching this paperwork and confirming their approval

Declaration

I certify that:

- Information requested is compatible with the stated purpose (section 4) and will not be used in anyway incompatible with that purpose.
- I understand information given on this form is correct.
- I understand that if any information given on this form is incorrect, I may be committing an offence under Section 170 Data Protection Act 2018.

Requestor

Signed:		**Date:**	

Authorising Officer

First name:		**Last name:**	
Job title:			
Signed:		**Date:**	

Where to send your request

Please note: If the form has not been fully or properly completed and authorised you will be asked to re-submit your application.

Please hand this form to a member of academy office staff to be submitted to the Data Protection Office, or send this form to:

Email: DPO@E-ACT.org.uk

Postal address: Data Protection Officer, E-ACT, Innovation Centre, Primley Avenue, Walsall, West Midlands WS2 9UA

Procedure for Police and other Organisation Requests for Information under Schedule 2 Part 1 Para. 2 Data Protection Act 2018

(Previously a request under Section 29 of the Data Protection Act 1998)

Introduction

Organisations that have a crime prevention, law enforcement or tax collection function may require personal information held by the Trust to prevent or detect a crime, or apprehend or prosecute an offender, or for taxation/ benefit purposes.

These organisations can submit requests under Schedule 2 Part 1 Para. 2:

- Police
- HM Revenue and Customs
- Child Support Agency
- Health and Safety Executive
- Official Receiver
- Solicitors or another acting on your client's behalf
- Solicitor acting on your client behalf, but asking for another's data
- Other Local Authorities or Public Bodies, acting under authorised powers.

The Trust may be able to release this information by applying an exemption under Schedule 2 Part 1 Para. 2 Data Protection Act 2018 (*previously a request under Section 29 of the Data Protection Act 1998*). There is no obligation on the Trust to do so and even if the exemption applies the Trust may decide that it should not release any information.

Please note that if the Trust has genuine concerns about releasing any personal information (for example, because it thinks it has other legal obligations such as the information being confidential) then it may ask for a Court Order requiring release of the information.

In the event that you receive a request from the police or any other organisation listed below, in the first instance you must ask for the appropriate form to be completed. Most organisations will have a standard form for this, the Trust's form is contained in the CCTV policy.

Receipt of a Request

Organisations wishing to request disclosure of personal information held by the Trust, must complete a "Request for Disclosure of Personal Data under Schedule 2 Part 1 Para. 2 Data Protection Act 2018' form".

If you receive a Request, please ensure you submit it without delay to our Data Protection Officer. All requests must be submitted either in person at one of our academies, for onward transmission to our DPO, or via email address: DPO@E-ACT.org.uk

Our DPO will keep a record of requests centrally and will share details of any requests, on receipt, with the relevant Regional Operations Director (ROD).

Completing the form

Section 1

- The name, job title (rank and collar number of police officer) and organisation name of the person making the request ('the Requestor') must be provided to enable us to identify that the person has statutory authority to make a request under the exemption.
- The address, a secure email address and a telephone number must be included to allow us to contact the Requestor or forward the information once a decision has been made.

Section 2

- Details of the specific information required and, where known, any other details which would enable us to locate the data e.g. location or person(s) the individual has had contact with, where the data is likely to be held or the dates when the individual was in contact with the Trust (*academy/regional office/national office*).
- Details of any additional documents which may help us to locate the information, or identify the data subject can be attached.
- For the purposes of crime prevention or apprehension/conviction of an offender the requested information should relate to a specific individual. This exemption must not be used for 'trawling' information and these requests **will be** refused.

Section 3

- Details of the offence. Where it is not possible to specify the offence, the appropriate box must be ticked. This should only be used where it is likely to prejudice the case as this information can aid the decision making process.
- Reason(s) why the information is necessary must be given.
- The Requestor must also state under what powers they are requesting the information. The Trust reserves the right to withhold data if sufficient grounds for applying an exemption are not provided.

Section 4

- The Requestor must state how they would like to receive the information. The most convenient, secure and preferred method is via secure password protected email.
- We can provide information by alternative means but this may result in delay releasing the requested information. If the Requestor wishes to collect the information, then we will require sufficient identification for example an ID badge or a warrant card.
- The Requestor must indicate the timescale in which the information is required. Dependent on the number received, volume and nature of the request it may take up to 5 working days to process.

When we receive a completed Request form we will assess whether or not this information will be released. We will endeavour to provide the information requested as soon as possible and will inform the Requestor if it is not possible to meet the required timescale.

Section 5

Once the Requestor has completed the form, it should be sent to us by secure email/post or in person.

The email address of the authorising officer should be included as confirmation.

For requests from the police the form must also be authorised by a person no lower than the rank of Police Inspector.

If the Trust does not consider the level of authorisation signatory to be sufficient we reserve the right to request further authorisation or to refuse to supply the information.

Failure to complete the form fully is likely to delay the process of obtaining the information.

Please note that the final decision to release the requested information is held by the Trust.

Contact Details:

Postal Address: Data Protection Officer, E-ACT Innovation Centre, Primley Avenue**,** Walsall**,** West Midlands WS2 9UA

Email: DPO@E-ACT.org.uk