

# Exmouth Community College



## **CCTV POLICY**

Policy Details	Date
Policy Written	Graham Allen/James Murphy
Policy Reviewed by Governors	Resources
Policy ratified by Governors	30.10.18
Review Cycle	Annually
Policy Review date	Autumn 1 2019

## 1 Policy Statement

- 1.1 Exmouth Community College uses Close Circuit Television (“CCTV”) within the premises of the Academy. The purpose of this policy is to set out the position of the Academy as to the management, operation and use of the CCTV at the Academy.
- 1.2 This policy applies to all members of our Workforce, visitors to the Academy premises and all other persons whose images may be captured by the CCTV system.
- 1.3 This policy takes account of all applicable legislation and guidance, including:
  - 1.3.1 General Data Protection Regulation (“GDPR”)
  - 1.3.2 Data Protection Act 2018 (together the Data Protection Legislation)
  - 1.3.3 CCTV Code of Practice produced by the Information Commissioner
  - 1.3.4 Human Rights Act 1998
- 1.4 This policy sets out the position of the Academy in relation to its use of CCTV.

## 2 Purpose of CCTV

- 2.1 The Academy uses CCTV for the following purposes:
  - 2.1.1 To provide a safe and secure environment for pupils, staff and visitors
  - 2.1.2 To prevent the loss of or damage to the Academy buildings and/or assets
  - 2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders
  - 2.1.4 To increase the perception of safety and reduce the fear of crime;

## 3 Description of system

- 3.1 [The system is a mix of 10 older analogue (eneo) cameras and 14 newer digital (Hik) cameras, 4 of these have fish eye capabilities. All images are stored on a Hikvision DVR. Most cameras record on a moving route whilst cameras overlooking the main drives are fixed. The system is serviced and maintained by Securi-guard South West.

- 4 Siting of Cameras
  - 4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
  - 4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Academy will make all reasonable efforts to ensure that areas outside of the Academy premises are not recorded.
  - 4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.
- 5 Privacy Impact Assessment
  - 5.1 Prior to the installation of any new CCTV camera, or system, a privacy impact assessment will be conducted by the Academy to ensure that the proposed installation is compliant with legislation and ICO guidance.
  - 5.2 The Academy will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.
- 6 Management and Access
  - 6.1 The CCTV system will be managed by the Principal.
  - 6.2 On a day to day basis the CCTV system will be operated by the Premises Manager
  - 6.3 The viewing of live CCTV images will be restricted to Site staff and those with significant pastoral responsibility for students (e.g SLT, Heads of Year).
  - 6.4 Recorded images which are stored by the CCTV system will be restricted to access by site staff and those with significant pastoral responsibility for students. On occasions teachers or support staff may be given access to aid with identification.
  - 6.5 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.
  - 6.6 The CCTV system is checked weekly by the Premises Manager to check correct operation.
- 7 Storage and Retention of Images
  - 7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

- 7.2 Recorded images are stored only for a period of roughly 28 days unless there is a specific purpose for which they are retained for a longer period.
- 7.3 The Academy will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
  - 7.3.1 CCTV recording systems being located in restricted access areas;
  - 7.3.2 Restriction of the ability to make copies to specified members of staff
- 7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Academy.

## 8 Disclosure of Images to Data Subjects

- 8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.
- 8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Academy's Subject Access Request Policy.
- 8.3 When such a request is made the Premises Manager and the DPO will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.
- 8.4 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Premises Manager and the DPO must take appropriate measures to ensure that the footage is restricted in this way.
- 8.5 If the footage contains images of other individuals then the Academy must consider whether:
  - 8.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;
  - 8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
  - 8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

- 8.6 A record must be kept, and held securely, of all disclosures which sets out:
- 8.6.1 When the request was made;
  - 8.6.2 The process followed by the Premises Manager and the DPO in determining whether the images contained third parties;
  - 8.6.3 The considerations as to whether to allow access to those images;
  - 8.6.4 The individuals that were permitted to view the images and when; and
  - 8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

## 9 Disclosure of Images to Third Parties

- 9.1 The Academy will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
- 9.2 CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
- 9.3 If a request is received from a law enforcement agency for disclosure of CCTV images then the Premises Manager must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.
- 9.4 The information above must be recorded in relation to any disclosure.
- 9.5 If an order is granted by a Court for disclosure of CCTV images then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

## 10 Review of Policy and CCTV System

- 10.1 This policy will be reviewed Annually
- 10.2 The CCTV system and any privacy impact assessments relating to it will be reviewed annually

- 11 Misuse of CCTV systems
  - 11.1 The misuse of CCTV system could constitute a criminal offence.
  - 11.2 Any member of staff who breaches this policy may be subject to disciplinary action.
- 12 Complaints relating to this policy
  - 12.1 Any complaints relating to this policy or to the CCTV system operated by the Academy should be made in accordance with the Academy Complaints Policy.

This policy is also compliant with General Data Protection Regulations.

