HOLYROOD
ACADEMY

POLICY

Academy Closed Circuit Television (CCTV)

(including Unmanned Aerial Vehicles - UAV)

Policy May 2018

Review May 2021

Throughout this document mention is made of video, video images or video system – this refers to images captured by either CCTV or UAV.

Introduction

1.1 Holyrood Academy uses closed circuit television (CCTV) images to reduce crime and monitor the Academy buildings to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to Academy property.

1.2 Holyrood Academy occasionally uses Unmanned Aerial Vehicles (UAV/Drones) in order to take publicity footage for prosepctus.

1.3 The system comprises of a number of fixed and dome cameras

1.4 The system has sound recording capability.

1.5 The CCTV system is owned and operated by the Academy and the deployment of which is determined by the Academy's leadership team. When using UAV the Academy will use the services of an external company specialising in this kind of work.

1.6 The CCTV is monitored centrally from the IT Office by the Network manager and his team of technicians. In addition the following departments monitor their own areas: Reception, D&T, Inclusion room, and Learning Centre.

1.7 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the Academy community.

1.8 The Academy's Video Schemes are registered with the Information Commissioner under Data Protection Act Regulations. The use of the video system, and the associated images and any sound recordings, is covered by Data Protection Regulations and the Protection of Freedoms Act 2012. This policy outlines the Academy's use of video systems and how they comply with these Acts.

1.9 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the Academy data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

2. Statement of Intent

2.1 The Academy complies with the Surveillance Commissioners Code of Practice. This can be seen at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf

2.2 The Academy also complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:
http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

2.3 CCTV warning signs will be clearly and prominently placed at all external entrances to the Academy, including Academy gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see Appendix B). In areas where CCTV is used, the

Academy will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

2.4 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

2.5 All uses of CCTV and UAV will be subject to the self-assessment tools from the Surveillance Commissioners site and have their own Privacy Impact Assessments.

3. Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The Academy will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

3.2 The Academy will make every effort to position cameras so that their coverage is restricted to the Academy premises, which will include outdoor areas.

3.3 CCTV will not be used in classrooms with the exception of the isolation unit, D&T computer room and Learning Centre. The Headteacher will be responsible for approving requests to add additional CCTV cameras in classrooms/communal rooms i.e. main hall.

3.4 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. Covert Monitoring

4.1 The Academy may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances authorisation must be obtained from a member of the senior management team.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

4.5 The Human Rights of all the people who use the Academy must be respected and covert monitoring must only be used as a last resort.

5. Storage and Retention of images

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded. The CCTV images will be kept for up to

30 days (in line with the purpose of recording this data) unless there is a current incident that is being investigated.

5.2 All retained data will be stored securely and will be listed on the Academys Data Asset Audit.

5.3 All retained data must be stored in a searchable system. Only a primary copy should be kept and secondary copies should only be created in exceptional circumstances, or when child safety is a concern.

6. Access to CCTV images

6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to video footage relating to themselves under the Data Protection Act. This may be refused or withheld if child safety is a concern.

7.2 All requests should be made in writing to the Headteacher or the Academys Data Protection Officer (see contact details below). Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The Academy will immediately indicate receipt and then respond within 30 calendar days of receiving the written request.

7.4 The Academy reserves the right to refuse access to video footage where this would prejudice the legal rights of other individuals, Child Protection, or jeopardise an ongoing investigation.

7.5 All attempts will be made to allow the viewing of the video, but if others can be identified (the blurring of faces should be considered) and their consent is not obtained, then selected still images may be provided. If still images continue to identify others then a transcript could be provided but the reasons for not releasing the videos and/or images must be recorded. This transcript might not meet the needs of the subject in requesting access.

7.6 The Academy should not provide copies of the video to others unless instructed to do so in law.

8. Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties' other than to authorised personnel such as the Police and service providers to the Academy where these would reasonably need access to the data (e.g. investigators) and with the correct authorisation.

8.2 Consideration should always be given to the safeguarding and best interest of the students. Data Protection should not be used as an excuse to prevent the viewing of images if there is an overwhelming need. All incidences and the reasons for release should be recorded.

8.3 Requests should be made in writing to the Headteacher or the Academy Data Protection Officer (see contact details below).

8.4 The data may be used within the Academy's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the Academy should be directed to the Headteacher or the Academy's Data Protection Officer in the first instance.

10. Complaints

10.1 The CCTV policy will be reviewed every three years unless a major change in national policy or system requires it to be reviewed earlier.

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this policy, please contact the Headteacher, via the Academy reception or our Data Protection Officer, Mr. I. Gover at dposchools@somerset.gov.uk

Appendix A - Checklist

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner.	Yes – August 2017	TC	August 2018
There is a named individual who is responsible for the operation of the system.	Yes – Ken Sealey (Network Manager	TC	If change of personnel
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	Yes	TC	On-going
Staff and members of the Academy community will be consulted about the proposal to install equipment.	Equipment already in place – not in classrooms	TC	If any changes to system necessary staff will be consulted
Cameras have been sited so that they provide clear images.	Yes	TC	On-going
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	Yes –positioned to capture premises.	TC	On-going
There are visible signs showing that the system is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	Yes – where sign not connected to the premises	TC	On-going review to ensure signage sufficient
Images from this system are securely stored, where only a limited number of authorised persons may have access to them.	Yes –limited to IT personnel, SLT or staff investigating incidences	TC	Reviewed in line with policy review
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	Yes – no more than 30 days unless investigation in progress	TC	In line with policy review
Except for law enforcement bodies, images will not be provided to third parties.	Agreed as per policy	TC	Reviewed in line with policy review
The organisation knows how to respond to individuals making requests for copies of their own images.	Yes – as laid down in the policy	TC	Reviewed in line with policy review
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Yes – daily monitoring takes place	TC	On-going

Appendix B – Signage

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Academy is to ensure that this requirement is fulfilled.

Where the CCTV sign is not attached to the property it should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the Academy
- The contact telephone number or address for enquiries

Images are being monitored and recorded for the purposes of crime prevention and public safety. This scheme is controlled by Holyrood Academy. For more information, call 01460 260100.