PENRYN COLLEGE

CCTV Policy

Approved by: Full Governing Body

Date approved: December 2022

Responsible SLT member: Operations Manager

To be reviewed: December 2023

Published: **Virtual School, School Website, Staff Handbook**

1 Policy Statement

1.1 Penryn College uses Close Circuit Television ("CCTV") within the premises of the college. The purpose of this policy is to set out the position of Penryn College as to the management, operation and use of the CCTV at the college.

1.2 This policy applies to all members of our Workforce, students and visitors to Penryn College's 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, but not limited to:

1.3.1 UK General Data Protection Regulation ("UKGDPR")

1.3.2 *[Data Protection Act 2018]* (together the Data Protection Legislation)

1.3.3 CCTV Code of Practice produced by the Information Commissioners Office (ICO)

1.3.4 Human Rights Act 1998

1.4 This policy takes into account other applicable Penryn College policies, including but not limited to:

1.4.1 Data Protection Policy

1.4.2 Code of Conduct for College Staff

1.4.3 Keeping Children Safe in Education

1.5 This policy sets out the position of Penryn College in relation to its use of CCTV.

2 Purpose of CCTV

2.1 Penryn College 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 college's buildings and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

3.1 The CCTV system comprises the following elements:

3.1.1 92 IP-based cameras running across the existing School network. These are a mixture of 4MP and 8MP resolutions, offering degrees of detail for different scenarios. Although offering audio capabilities it is currently not planned to utilise this feature. Should this be deemed a necessary requirement in the future this policy will be amended to reflect this, with accompanying changes to the other associated policies, all stakeholders informed of the changes and site signage amended accordingly.

3.1.2 A network-based 128 Channel Network Video Recorder (NVR) with sufficient hard drive capacity to store up to 30 days of video footage and store / replay / export video at a resolution suitable for the uses stated in this policy.

3.1.3 Appropriate site signage used to clearly inform all staff, students and visitors of the presence and justifications for use of the CCTV system.

3.1.4 Clearly defined lists of staff with direct and indirect access, coupled with an access log and incident register to be completed by anyone accessing the system.

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. Penryn College will make all reasonable efforts to ensure that areas outside of the college premises are not recorded, including the use of software-based 'blanking' of, for example, windows of surrounding houses.

4.3 Signs will be erected in key locations to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

4.5 Cameras will not be sited in classrooms

5 Privacy Impact Assessment

5.1 Prior to the installation or upgrade of any CCTV camera or system a privacy impact assessment will be conducted by Penryn College to ensure that the proposed installation is compliant with legislation and ICO guidance. The current assessment (Appendix A) was carried out in January 2022 to help inform the specification for the CCTV refresh carried out in July / August 2022

5.2 Penryn College will adopt a privacy by design approach when installing new cameras or upgrading existing 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 Systems and Technologies Strategic Manager.

6.2 On a day to day basis the CCTV system will be operated by named members of the teams listed in 6.3

6.3 The viewing of live CCTV images will be restricted to members of SLT, the EST team, designated pupil support staff, employed Security staff and the Systems and Technologies Strategic Manager.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by members of SLT, the EST team, designated pupil support staff, the Systems and Technologies Strategic Manager and the police / law enforcement agencies (in the event they require evidence for ongoing investigations).

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 unless supervised by an SLT member or the Systems and Technologies Strategic Manager.

6.6 The CCTV system will be checked weekly to ensure it is operating correctly by the Systems and Technologies Strategic Manager. Any issues discovered will be either actioned internally where possible or raised with the incumbent support company.

6.7 All access to the live or stored images will be recorded in an access log, to include person(s) accessing, date and time, reason for access, any export of images or video and destination of these files

6.8 The handling of all live and recorded material will be in accordance with the school's Staff Code of Conduct Policy and specifically the section regarding confidentiality.

6.9 All staff involved in accessing or viewing CCTV data must sign and date the CCTV Confidentiality Agreement, a copy of which must be held on record by HR

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 30 days unless there is a specific purpose they are retained for a longer period, for example should the police require evidence in an ongoing investigation.

7.3 Penryn College 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 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to view footage and / or make copies to specified members of staff. Names to be recorded in the access log as approved for access.

7.3.4 All cameras to have tamper alarms as standard

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 Subject Access Request section of Penryn College's Data Protection Policy.

8.3 When such a request is made either SLT or the Systems and Technologies Strategic Manager 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. SLT or the Systems and Technologies Strategic Manager 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 Penryn College 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 SLT or the Systems and Technologies Strategic Manager 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 Penryn College 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 either SLT or the Systems and Technologies Strategic 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 the privacy impact assessment relating to it will be reviewed annually.

11 Misuse of CCTV systems

11.1 The misuse of the 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 Penryn College should be made in accordance with the college's Complaints Policy.

APPENDIX A - CCTV PRIVACY IMPACT ASSESSMENT

1 Who will be captured on CCTV?

Pupils, staff, parents / carers, volunteers, Governors and other visitors including members of the public.

2 What personal data will be processed?

Facial Images, behaviour, clothing and personal apparel, vehicle details (on school site only).

3 What are the purposes for operating the CCTV system? Set out the problem that the School is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

Tracking / tracing of very vulnerable students with proven history of eluding adult supervision *Prevention or detection of bullying or other acts of aggression between 2 or more parties* *Prevention or detection of crime* *Prevention or detection of damage and/or vandalism*

4 What is the lawful basis for operating the CCTV system?

Legal Obligation (especially Keeping Children Safe in Education legislation), legitimate interests of the organisation to maintain health and safety, reduce strain on public monies due to excessive repairs and to prevent and investigate crime.

5 Who is/are the named person(s) responsible for the operation of the system?

The Systems and Technologies Strategic Manager

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

b. siting of the cameras and why such locations were chosen;

c. how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

d. where signs notifying individuals that CCTV is in operation are located and why those locations were chosen;

e. whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

Cameras have been chosen based on the best available current technologies providing clarity of images mapped to specific need in each area. Medium resolution cameras (4MP) will be used in general areas for person tracking, group monitoring and basic identification and high quality (8MP) ones in areas at greatest risk of break-in (unpermitted ingress to site or buildings) allowing for the potential to identify individuals accurately.

The recording equipment has been chosen based on quality of image it is able to process (including high quality playback), sufficient storage to enable agreed retention periods and modern technologies that allow for features such as face and vehicle differentiation (Deep Learning technology)

For the purposes of safeguarding cameras have been placed in such positions as there are no 'deadspots' (areas where vulnerable students can go to avoid detection). To help law enforcement agencies points of ingress to the site and building will be covered by higher quality cameras to allow for facial recognition to be carried out.

Cameras are sited to only capture, as far as practicable, movements around the school site. where there is a possibility of capturing images outside of the school site without people's knowledge obfuscation technologies will be used to prevent this

At a minimum notification signs will be located at each public entrance to the site (front and back gates) in a prominent position and clearly visible. They will be kept clear of obstructions such as seasonal foliage and will be checked regularly to ensure they are still clear and readable. Additional reminder signs may be placed at other strategic internal positions at some point.

Redacting of third-party data is possible through the Hikvision iVMS software used in combination with video editing software

7 Set out the details of any sharing with third parties, including processors

Police access to any footage required in ongoing investigations

Subject access requests by visitors, parents etc. when involved in internal investigations (eg. student bullying accusations, abuse of school staff by parents)

Viewing of footage by the support company when servicing and maintaining systems or troubleshooting issues as part of the support contract. It will be made clear that this will not be taken off-site by any method.

There will be no external access to the systems at any time.

8 Set out the retention period of any recordings, including why those periods have been chosen

Recordings will be kept for 30 days to allow any potential incident investigations to be carried out.

In the event the Police require footage for evidence this will be exported to secured / encrypted media by someone with agreed access to the system and all details recorded in the access and event log

9 Set out the security measures in place to ensure that recordings are captured and stored securely

The NVR is mounted in the school main server room, which is secured using maglock and key access. Access to live views and recordings is restricted to named individuals and all access is recorded. Devices and software used are password protected to ensure access is controlled. Cameras are all mounted at a height sufficient to deter casual interference and all have tamper monitoring as standard.

10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

For example:

- Is it fair to record them in the way proposed?

  Monitoring and recording will be used to ensure mutual safety and protection of users of the school, as well as the security of the school site.

- How is the amount of data processed to be minimised?

Recording retention periods will be restricted and in low-risk areas cameras will be set to only activate based on movement or IR triggers, especially at night.

- What are the risks of the system being accessed unlawfully?

  Very low. Main risks would be around unauthorised people getting access to the server room. sharing of log in information or leaving internal remote connection systems logged in and devices left lying around in public areas

- What are the potential data breach risks?

  Extremely low risk of 3rd parties accessing recorded data and making this available outside of the school. Sharing of data with others in breach of school policies and without following rules in place

- What are the risks during any transfer of recordings, or when disclosed to third parties such as the police?

  Loss of transfer device, interception of data during transfer, insufficient data protection at receiving end

11 What measures are in place to address the risks identified?

Signage, policies and notifications will be used to inform everyone on the school site that they are being constantly monitored and recorded. Who to contact with any queries will be clearly stated on the signage.

Checks will be made regularly to ensure retention periods are not being exceeded and remedial action taken where necessary.

All recording equipment is secured in a lockable room. All cameras have tamper alarms.

Any portable media used to transport stills / footage will be password protected / encrypted

Internal remote access systems (eg. IPads for SLT) to be PIN and password controlled. Software will be set to log out after a period of inactivity.

*There will be **no** external access to the systems.*

School policies are in place and clear in the expectations of school staff in relation to Data Protection and handling as well as the expectations of compliant and professional staff behaviour.

12 Have parents and pupils where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

There has been no new consultation carried out as the school has had CCTV in place for 14 years. We will, however, inform parents of the upgraded system and direct them to the school website for policies and further information.

13 When will this privacy impact assessment be reviewed?

January 2023

Approval:

This assessment was approved by the Data Protection Officer:

DPO ……

Date …….

APPENDIX B – CCTV Confidentiality Agreement (to be signed by all staff accessing the CCTV systems)

CCTV confidentiality agreement

This confidentiality agreement is entered into by and between Penryn College and the staff member accessing the CCTV system for the purpose of preventing the unauthorised disclosure of confidential information in line with your duties to protect personal information, under the UK GDPR and the Data Protection Act 2018.

For the purpose of this agreement, "confidential information" will include all live and recorded camera footage that constitutes personal information under the UK GDPR showing any pupil, parent, member of staff or visitor to the school, or has or could have value, commercial or otherwise, in the business in which the disclosing party is engaged.

I declare that I will only share or disclose information regarding the school with other named professionals who have a legitimate need to know about it. I will, therefore:

- Not disclose confidential information to any unauthorised person without the subject's consent.
- Act in good faith at all times in relation to the disclosure of confidential information.
- Not post confidential information regarding pupils, staff, parents or other stakeholders on social medial; nor will I contribute to discussions on social media regarding the school or anyone associated with it.
- Assure that conversations of a sensitive nature regarding pupils, parents, staff, volunteers or other stakeholders that arise from accessing the CCTV footage only take place in a private space and with appropriate individuals who have been authorised to know the information.
- Ensure that all footage I access is handled in line with the Data Protection Policy and the School CCTV Policy, and that I am thorough and careful when it comes to securing and erasing data.
- Maintain accurate records of access with all relevant detail as dictated by the CCTV Policy
- Undergo any relevant data protection training the school deems necessary for my role.
- Not disclose any information, or partake in any discussions with unauthorised individuals, about ongoing investigations into allegations against staff members, volunteers, governors or stakeholders.
- Be fully aware that other staff, volunteers or stakeholders may have connections within the school and may overhear conversations of a sensitive nature.
- Uphold the good name and reputation of the school at all times; inside and outside of school.

I am aware that confidentiality obligations must not prevent me from sharing necessary information for the purposes of keeping children safe and promoting their welfare, and that I am protected under the Public Interest Disclosure Act with regards to sharing confidential information for the purposes of whistleblowing – I am aware that nothing in this agreement precludes the sharing of information to this effect.

I will hold and maintain the confidential information in strictest confidence for the sole and exclusive benefit of the school; therefore, I will not, without prior approval of the school, use for my own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of the school, any confidential information.

I have read and understood the school's Staff Code of Conduct Policy and will act in accordance with this policy at all times.

By signing this agreement, you are agreeing to your duty to hold confidential information in confidence – this will remain in effect until the information no longer qualifies as confidential, or until the school sends written notice releasing you from this agreement, whichever occurs first.

Please retain a copy of this agreement and give a signed copy to the HR office. If you have any questions or concerns, please contact HR or your SLT link.

Name of individual	
Role	
Signed	
Date	
Name of Authoriser	
Role	
Signed	
Date	