CCTV MANAGEMENT POLICY 2024

HARTPURY

1. **Purpose**

1.1. The purpose of this policy is to regulate the management, operation and use of the image only, CCTV system at Hartpury. Cameras are in continual operation and will be used if required to monitor activities within buildings on the Hartpury estate, car parks and other public areas to identify criminal activity occurring, anticipated or perceived, and for the purpose of securing the safety and wellbeing of Hartpury buildings, staff, students and visitors. Live monitoring of the CCTV system will be restricted to public and communal areas if necessary and proportionate. Under exceptional circumstances, CCTV may be monitored in live time in order to safeguard students, staff and visitors to the Hartpury campus.

1.2. Automatic Number Plate Recognition (ANPR) is used at the main entrance to the Hartpury campus and any references to CCTV throughout this document also apply to ANPR.

1.3. CCTV monitoring and recording systems will only be installed in or on Hartpury property when reviewed by the Hartpury Campus Security Team and approved by a member of SMT.

1.4. The system comprises a number of fixed and functional (Pan/Tilt/Zoom) cameras located in the majority of buildings including residential accommodation and externally appropriate locations across the campus grounds. These are monitored by appropriately trained staff who are all required to read the CCTV policy.

1.5. Hartpury's use of CCTV complies with the requirements of the Data Protection Act and where applicable, the Regulation of Investigatory Powers Act 2000. Hartpury is registered with the Information Commissioner Office as a Public Authority.

1.6. This policy document will be subject to review annually to include consultation with stakeholders as appropriate.

1.7. The CCTV system is owned by Hartpury University & College.

1.8. Independently installed and operated CCTV systems by staff/students will not be permitted on Hartpury campus property and where found to be the case, actions will be taken to discontinue the use of unauthorised systems.

2. Objectives

Hartpury is committed to the safety and security of all campus users and property. This policy is to assist in the prevention and detection of crime.

2.1 To facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.

2.2 To protect Hartpury property.

2.3 To provide a safer environment for students and other campus users in respect of Safeguarding.

2.4 To support the Police to prevent and detect crime, by providing evidence if appropriate to support an enquiry or prosecution.

2.5 To assist with the identification of actions that may result in Behaviour Management investigations involving students or HR investigations in respect of staff disciplinary matters.

2.6 To monitor and assist with Campus traffic management.

2.7 To reduce the fear of crime and to provide reassurance to students, staff and visitors.

3. Management of the CCTV System

3.1 The CCTV operation will be administered and managed by the Head of Safeguarding, Wellbeing and Health or nominated person in accordance with the principles and objectives expressed in the policy document.

3.2 Staff access is restricted to the Safeguarding and Wellbeing Management Team, Residential Support Team, Facilities department and IT (both for system maintenance). The Head of Safeguarding, Wellbeing and Health or nominated person will review access rights on an annual basis. All staff users must be approved and authorised by a member of the Senior Management Team and the Head of Safeguarding, Wellbeing and Health or their nominee. In exceptional circumstances, access can be approved by a member of the Senior Management Team or the Head of Safeguarding, Wellbeing and Health.

3.3 Unauthorised persons will not be permitted to access the system at any time.

3.4 The day-to-day management of the CCTV system will be the responsibility of the Head of Safeguarding, Wellbeing and Health or nominated person supported by the Residential Support Team.

3.5 Cameras will be monitored by authorised staff using Milestone software which will be maintained by the IT Department.

3.6 CCTV will be in operation 24 hours a day, 365 days of the year. Live viewing will only be undertaken if necessary and proportionate.

3.7 If out-of-hours emergency maintenance is required, the IT Support Emergency Help Line will be contacted.

3.8 CCTV notification signs, as required by the Code of Practice of the Information Commissioner, will be placed at all access routes to areas covered by the CCTV.

3.9 Liaison meetings may be held with all internal and external agencies involved in the support of the system when necessary.

3.10 System Control – Monitoring Procedures

3.10.1 On a daily basis, the Head of Safeguarding, Wellbeing and Health and the Residential Support Team will check and confirm the efficiency of the system. The Head of Safeguarding, Wellbeing and Health or nominated person will undertake monthly checks on all residential building CCTV ensuring that:

- the cameras are functional
- the equipment is properly recording
- the field and angles of view are capturing imagery as intended

3.10.2 Access to the CCTV will be strictly limited to the Residential Support Team Staff and their management and specific authorised persons as described in 3.2.

3.10.3 An annual review of CCTV DPIA's will be undertaken by the Head of Safeguarding, Wellbeing and Health.

3.10.4 Unless an immediate response to events is required, operators must not redirect cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained from the Head of Safeguarding, Wellbeing and Health or nominated person for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

3.10.5 Recording is carried out on digital data apparatus as described in 4.1.1. This equipment is located within the IT department.

3.10.6 Recorded data will only be released to the media for use in the investigation of a serious crime and only with the written authority of the Police. Recorded data will never be released to the media for purposes of entertainment.

3.11 Exemptions

3.11.1 The CCTV is designed to ensure maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover all parts of the campus and wider areas and/or detect every single incident taking place.

3.12 Retention and disposal of material

3.12.1 Footage will be stored on data recorder hard drives for up to 30 days.

3.12.2 Footage will be provided on a USB device if requested by selected, appropriate external agencies for the purpose of detecting crime and for the prosecution of offenders in accordance with GDPR.

3.12.3 All still photographs and hard copy prints will also be securely disposed of as

confidential waste.

4. Digital Recording Procedures

4.1. Rules for retention of data

4.1.1 In order to maintain and preserve the integrity of the Network Video Recorders (NVR), servers store recordings on hard disks used protected with Raid technology and encryption. For recording events from the surveillance cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to.

4.1.2 Each NVR must be identified by a unique mark or serial number. This is maintained by the IT department.

4.1.3 Each DVR must be kept in a secure location with access restricted to authorised staff.

4.1.4 The Head of Head of Safeguarding, Wellbeing and Health, in liaison with the IT department, shall check daily to ensure the system is operational.

4.1.5 A disk required for evidential purposes must be of the CD-R type or USB storage only, both will be provided in pairs each carrying an identical identification number, one a Master to be retained by Hartpury, the other a copy which can be released to the police or other authorised third party on production of a signed data access request form.

4.1.6 The disk / USB should be loaded with the required CCTV data and viewer programme; identical information should be loaded on both Master and copy disks / USB.

4.1.7 Each disk / USB should be sealed in its own case; the Master Copy should be kept in a secure storage drawer. The Copy disk / USB is handed to the person making the request on production of positive ID such as Police Warrant Card or Agency Picture ID Card.

4.1.8 The record sheet should then be completed, and the Copy disk signed for and counter signed by the Head of Safeguarding, Wellbeing and Health or nominated person.

4.1.9 All captured CCTV footage relating to an investigation will be stored as long as such a time it is no longer required e.g. completion of any investigation or formal process.

Permanent deletion will be the responsibility of the Head of Safeguarding, Wellbeing and Health.

4.2. Dealing with official requests: use of CCTV for the detection of criminal activities

4.2.1 CCTV recorded images may be viewed by the Police for the purpose of prevention and detection of crime.

4.2.2 Other reason for which CCTV may be used:

- CCTV recorded images may be viewed by authorised officers of Hartpury for supervisory purposes.
- CCTV recorded images may be viewed by authorised officers of Hartpury for the investigation of discipline matters.
- Authorised demonstration and training.
- For immediate action relating to live incidents, e.g. an immediate pursuit.
- For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings).
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- For any major incidents.

4.2.3 A record will be maintained of the release of Data on Disk / USB to the Police or other authorised applicants. A register will be available for this purpose.

4.2.4 Viewing of CCTV images by the Police must be recorded in writing and entered in the log book. This will be under the management of the Head of Safeguarding, Wellbeing and Health. Requests by the Police will only be actioned under section 29 of the Data Protection Act 2018.

4.2.5 Should a disk / USB be required for evidence; a copy may be released to the Police under the procedures described in paragraph 4.1.5-4.1.8 of this policy. Disks / USB will only be released to the Police on the clear understanding that they remain the property of Hartpury, and both the disk / USB and information contained on them are to be treated in accordance with this policy.

4.2.6 Hartpury retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained therein unless a Court order is produced to the contrary.

4.2.7 The Police may require that Hartpury retain the stored disk(s) / USB for evidential purposes. Such disk(s) will be properly indexed and securely stored under the management of the Head of Safeguarding, Wellbeing and Health or nominated person until required by the Police.

4.2.8 Applications received from other agencies than the Police (e.g. solicitors) to view or release disks will be referred to the Head of Safeguarding, Wellbeing and Health. In appropriate circumstances data will normally be released where satisfactory documentary evidence is produced to show that they are required for legal proceedings, or in response to a Court Order. A fee may be charged in such circumstances.

5. Staff

5.1 All staff that are required to operate CCTV system are required to have read and understood this policy.

5.2 Only authorised staff will have access to CCTV images.

5.3 The Head of Safeguarding, Wellbeing and Health or nominated person will ensure that all staff required to operate the CCTV system are trained in respect of all relevant

operational, legal and administrative functions arising in respect of CCTV operation, including mandatory Hartpury information compliance testing.

6. Breaches of the policy – including breaches of security

6.1 Any breach of this policy by authorised users will be initially investigated by the Head of Safeguarding, Wellbeing and Health or appropriate line manager, in order for appropriate disciplinary action in liaison with HR.

6.2 Any serious breach of the policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

7. Assessment of the scheme

7.1 Performance monitoring, including random operating checks, may be carried out by the Head of Safeguarding, Wellbeing and Health or nominated person.

8. Access by the data subject

8.1 The Data Protection Act provides Data Subjects (individuals to whom personal data relate) with a right to access data held about themselves, including that obtained by way of the CCTV system.

8.2 Requests for information, including Data Subject Access Requests, should be sent to Gillian Steels, Clerk to the Corporation Gillian.Steels@hartpury.ac.uk 01452 702159.

9. Complaints and Contacts

9.1 The Head of Safeguarding, Wellbeing and Health is responsible for the operation of the CCTV system, and compliance with this policy. Any concerns in respect of the system's use or compliance with this policy should be addressed to the Head of Safeguarding, Wellbeing and Health and/or the Hartpury Complaints Policy and Procedure.

9.2 Any concerns about the CCTV system should be addressed to the Head of Safeguarding, Wellbeing and Health or appropriate line manager.

9.3 Complaints will be investigated in accordance with the Hartpury Complaints Policy and Procedure.

9.4 Contacts:

Head of Head of Safeguarding, Wellbeing and Health/DDSL/Prevent Lead

01452 702495

Rayna.Edwards@hartpury.ac.uk

Deputy Principal – Resources/DSL

01452 702459

Lesley.Worsfold@hartpury.ac.uk

Head of IT

01452 702626

Matthew.Reeve@hartpury.ac.uk

Related documents

1. General Privacy Policy
2. Acceptable Use Policy
3. Accommodation Licence (College & University Students)
4. Residential Handbook (College & University on campus residential students)

Equality, Diversity & Inclusion

As with all Hartpury policies and procedures, due care has been taken to ensure that this policy is appropriate to all members of staff and students regardless of their age, disability, ethnicity, gender, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sexual orientation and transgender status.

The policy will be applied fairly and consistently whilst upholding Hartpury's commitment to providing equality to all. If any employee feels that this or any other policy does not meet this aim, please contact the HR Department.

Approval and Review Cycle

Date Last Approved	November 2024
Policy Owner	Head of Safeguarding, Wellbeing and Health
Approving Committee	SMT/Executive
Status	APPROVED
Effective from	November 2024
Next Review Date	August 2026