Surveillance Policy

1. Policy

1. This Policy governs the installation and operation of all Closed Circuit Television (CCTV) cameras, Automatic Number Plate Recognition (ANPR) systems and Body Worn Video (BWV) systems at the University of York (University).
2. This policy applies to all University employees, engaged sub-contractors and any persons on University premises.

2. Purpose

1. The University uses CCTV, ANPR and BWV, hereafter collectively referred to as surveillance systems, to:

- *monitor and collect visual images for the purposes of security and the prevention and detection of crime.*

3. Pre-Installation

1. The University is committed to balancing the need to use surveillance against the right of individuals to a private life and will always consider alternative, less privacy intrusive, solutions before installing or renewing any surveillance system.
2. As part of that review process, a Privacy Impact Assessment (PIA) will be undertaken by representatives from the business area proposing installation or renewal with support from the University's Security Manager (SM).
3. Where surveillance equipment borders non-university land, the relevant landowner will be consulted as part of that assessment and any agreed actions incorporated into the PIA.
4. The PIA will be considered for approval by the University's Director of Health, Safety and Security (DHSS) in consultation with the University's Security Manager and Information Governance Officer (IGO).
5. The SM is responsible for retaining on file a copy of all completed PIAs submitted under 3.2 above for approval.
6. In cases where designated use of the area changes, a second PIA should be undertaken by the relevant business area, again with support from the SM, and submitted to the DHSS for review.

4. Installation

1. Surveillance equipment must be carefully selected, in consultation with the SM, to ensure it is of sufficient quality to record footage able to support the chosen purpose.
2. In addition, equipment must be carefully positioned to:

- *cover the specific area to be monitored only;*
- *keep privacy intrusion to a minimum;*
- *ensure that recordings are fit for purpose and not in any way obstructed (e.g. by foliage);*
- *minimise risk of damage or theft.*

5. Operation and storage

1. The University must avoid dependency on a key individual to operate surveillance systems and should make arrangements to ensure adequate cover is in place.
2. Where controllable cameras are used, operators must only target recordings where there is reasonable suspicion that an individual or individuals are involved in nefarious activities.
3. Cameras must not be used to view into private property and operations staff must be mindful of student privacy within accommodation blocks.
4. BWV equipment must be worn in a prominent position and at chest height. It should only be used where Patrol Officers believe they are likely to be subject to verbal and/or physical abuse or intimidation.
5. All surveillance system footage must be recorded centrally on University servers or transferred to secure servers at the end of shift. The Health, Safety and Security Department is responsible for working closely with colleagues in IT Services to ensure chosen systems are appropriate.
6. All surveillance system recordings should be viewed in secure private offices and made available to authorised personnel only.
7. Viewing monitors should be password protected and switched off when not in use to prevent unauthorised use or viewing.
8. The SM should undertake an annual check to establish that those individuals with surveillance system access rights continue to require viewing permissions. An annual report should be made available to the DHSS. In addition, job exit procedure should include arrangements for revoking access to surveillance systems where viewing rights are no longer required.

6. Signage and verbal communication

1. Signs will be displayed at campus entrance/exit points and in areas of strategic importance and will communicate:

- *that monitoring and recording is taking place;*
- *who the system owner is;*
- *where complaints/questions about the systems should be directed.*

2. The University has produced a standard surveillance notice for use on campus.
3. The Head of Estates Operations is responsible for ensuing signage is installed at appropriate locations across the University estate and for its continual maintenance.
4. In addition, for BWV systems, Patrol Officers will, where possible, make a verbal announcement of their intention to use audio and video recordings before turning on the equipment.
5. Once recording, a further announcement should be made, again where possible, to cover:

- *why the recording has been activated;*
- *date, time and current location.*

6. When communicating with the public, all announcements should be made using clear language.

7. Covert surveillance

1. Covert surveillance will be used in a limited number of cases where:

- *an active investigation is underway;*
- *there are clear grounds for suspecting criminal activity;*
- *alternative options to surveillance have been considered and deemed ineffective;*
- *overt surveillance would impede the effectiveness of monitoring;*
- *the use of surveillance is unlikely to cause excessive privacy intrusion.*

2. Before covert surveillance is installed, prior written approval of the University's DHSS and Registrar and Secretary must be obtained.
3. Where covert surveillance is authorised, its use must cease as soon as any active investigation has concluded.

8. Disclosure

1. Where an individual requests access to his/her own personal information held in the University's surveillance system, the request will be handled centrally by the IGO in line with University process.
2. On receipt of a 3rd party request for access to surveillance footage, the SM and/or his/her representative will consider release and liaise with the IGO as appropriate.
3. The SM is responsible for ensuring a full record is maintained of all 3rd party requests. This log should capture:

- *date of request;*
- *name of requester;*
- *name of organisation requesting information;*
- *a brief description of the information sought;*
- *the legal exemption relied on;*
- *details of the University's decision;*
- *date or decision and/or release;*
- *name of the authorising officer.*

4. Where 3rd party disclosures are made outwith core business hours, a full record of release must be maintained and, where appropriate, relevant forms retrospectively completed.
5. Before disclosing any footage, consideration should be given to whether images of third parties should be obscured to prevent unnecessary disclosure.
6. Where information is disclosed, the disclosing officer must ensure information is transferred securely. For further information on secure transfer, see, https://www.york.ac.uk/it-services/security/encryption/#tab-2.
7. Images may be released to the media for purposes of identification. Any such decision to disclose will be taken in conjunction with the Police and/or other relevant law enforcement agencies.
8. Surveillance recordings must not be further copied, distributed, modified, reproduced, transmitted or published for any other purpose.

9. Training

1. All staff are required to receive training in the use of surveillance systems and relevant legislation before they are granted access to any system or surveillance footage.
2. Training will be delivered by the Health, Safety and Security (HSS) Department with input from the University's IGO.
3. In addition, the Security Manager is expected to stay abreast of developments in the field of surveillance and disseminate best practice to all relevant personnel as appropriate.

10. Retention and disposal

1. Typically, surveillance recordings shall be retained for a maximum of 31 calendar days following capture and will be securely overwritten or destroyed after this time.
2. Where surveillance recordings are requested as part of an active investigation, they will be protected against loss or held separately from the surveillance system. These records will be retained for 6 months following date of last action and then disposed of as per 9.1 above.
3. Once hardware has reached the end of its active life, DHSS will work with the University's IT Services to ensure safe disposal in line with best Data Protection practice.

11. Complaints

1. Complaints and enquiries about the operation of the University's surveillance system should be sent to the University's DHSS for action.
2. Where appropriate, allegations or complaints will be investigated under the University's normal grievance procedures.
3. Non-standard requests relating to the University's surveillance system will be handled centrally under the terms of the Freedom of Information Act, 2000. For further information see, https://www.york.ac.uk/records-management/foi/foi-policy/.

Scope

This policy governs the installation and operation of all Closed Circuit Television (CCTV) cameras, Automatic Number Plate Recognition (ANPR) systems and Body Worn Video (BWV) systems on University of York premises.

This policy applies to all University of York employees, engaged sub-contractors and extends to any persons on the University of York site.

Oversight

The Information Security Board, chaired by the Director of Information, together with the Director of Health, Safety and Security will monitor the effectiveness of this policy and carry out regular review, at least on an annual basis.

Responsibilities

Overall responsibility lies with the Director of Health, Safety and Security.

Day-to-day responsibility is as follows:

- Security Manager
- Any individual wishing to install or renew a surveillance system on the University site.

Document History

Date Approved by Information Security Board

Review

Review cycle: Two years
Date of next review: 01 May 2019