Surveillance Policy

Purpose

1. The University uses CCTV, ANPR, BWV and DAC technologies, hereafter collectively referred to as surveillance systems, for the purposes of security and the prevention or detection of crime.

2. The University is committed to ensuring its use of surveillance technologies is lawful, fair, and transparent and complies with all other standards set out in data protection law. This policy sets out the University's procedure for approving and operating the use of such technologies.

Scope

3. This policy relates to the installation and use of surveillance technologies centrally managed by the University's Campus Safety Team.

4. This policy does not extend to the local installation of video or audio and video recording technologies e.g., webcams installed in laboratories to monitor equipment or record experiments; cameras used to monitor teaching spaces; drone technologies where cameras are used and dash cams installed in University of York owned or leased vehicles. These installations are governed by the Policy for the Management and Operation of Local Surveillance Technologies.

5. This Policy applies to all University employees, engaged sub-contractors and any persons on University premises.

Definitions

6. Surveillance technologies include all Closed-Circuit Television (CCTV) cameras, Automatic Number Plate Recognition (ANPR) systems, Body Worn Video (BWV) systems and Door Access Control (DAC) technologies in use at the University.

Policy statement

7. Pre-installation

    7.1. 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.

    7.2. As part of that review process, a Data Protection Impact Assessment (DPIA) will be undertaken by representatives from the business area proposing installation or renewal with support from Campus Safety.

    7.3. Where surveillance equipment borders non-University land, the relevant landowner will be consulted as part of that assessment.

7.4. The DPIA will be submitted to the University's Data Protection Officer for approval.

7.5. In cases where designated use of the area changes, the existing DPIA will be revisited and resubmitted to the Data Protection Officer for approval.

8. Installation

8.1. Surveillance equipment will be carefully selected, in consultation with Campus Safety, to ensure it is of sufficient quality to support the chosen purpose.

8.2. In addition, video-based equipment will 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.

9. Operation and storage

9.1. The University will avoid dependency on a key individual to operate surveillance systems and will make arrangements to ensure adequate service cover is in place.

9.2. Where controllable cameras are used, operators must only target recordings where there is reasonable suspicion that an individual or individuals are involved in unlawful, unconscionable or reckless activities.

9.3. Cameras must not be used to view into private property or student rooms in college accommodation blocks.

9.4. BWV equipment must be worn in a prominent position at chest height whenever a patrol officer is attending an incident or anticipates being subjected to verbal abuse, physical assault, or intimidation.

9.5. All video footage must be recorded centrally on University servers or transferred to secure servers at the end of shift.

9.6. All video recordings should be viewed in secure private offices and made available to authorised personnel only.

9.7. Viewing monitors should be password protected and switched off when not in use to prevent unauthorised use or viewing.

9.8. The Campus Safety Team should undertake an annual check to establish that those individuals with surveillance system access rights continue to require viewing permissions. In addition, job exit procedures should include arrangements for revoking access to surveillance systems where viewing rights are no longer required.

10. Signage and verbal communication

10.1. Signs will be displayed at campus entrance/exit points and in areas of strategic importance and will communicate using clear language:

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

10.2. The University has produced a standard surveillance notice for use on campus.

10.3. The Head of Estates Operations is responsible for ensuring signage is installed at appropriate locations across the University estate and for its continued maintenance.

10.4. In addition, for BWV systems, Patrol Officers will, where possible, make a verbal announcement of their intention to use audio and video recording before turning on the equipment.

10.5. Once recording, a further announcement should be made, again where possible, to cover:

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

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

11. Covert surveillance

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

- an active HR 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; and
- the use of surveillance is unlikely to cause excessive privacy intrusion.

11.2. Before covert surveillance is installed, prior written approval of the University's Vice Chancellor must be obtained.

11.3. Covert surveillance must not be used in areas where a person would reasonably expect privacy (such as toilets or changing rooms). Nor should it capture communications that individuals would expect to be treated as private.

11.4. A specific Data Protection Impact Assessment must be undertaken in respect of the covert surveillance.

11.5. If third-parties are used, the University must have a contract with them to ensure their compliance as data processor pursuant to Article 28 of the UK General Data Protection Regulation.

11.6. Where covert surveillance is authorised, its use must cease as soon as any active investigation has concluded.

12. Disclosure

12.1. Where an individual requests access to their own personal information held in the University's surveillance system, the request will be handled centrally by the Information Governance Team in Legal Services in line with University processes.

12.2. During core hours, Legal Services will manage third-party requests for access to surveillance footage, consulting with Campus Safety as appropriate.

12.3. Outside core hours, Campus Safety will manage time-critical third-party requests for access to surveillance footage.

12.4. Legal Services and Campus Safety are responsible for ensuring a full record is maintained of all third-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 of decision and, if applicable, date of release;
- name of the authorising officer.

12.5. Before disclosing any footage, consideration should be given to whether images of third parties should be obscured to prevent unnecessary disclosure.

12.6. Where information is disclosed, it must be transferred securely in accordance with the University's Information Classification and Handling Scheme.

12.7. Surveillance recordings must not be further copied, distributed, modified, reproduced, transmitted, or published for any other purpose.

13. Training

13.1. Authorised personnel 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.

13.2. Training will be delivered by the Campus Safety Team with support from the Information Governance Team in Legal Services where required.

14. Retention and disposal

14.1. 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.

14.2. 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 six months following the date of last action and then disposed of as per 14.1 above.

14.3. Once hardware has reached the end of its active life, the Campus Safety Team will work with the University's IT Services to ensure safe disposal in line with best data protection practice.

15. Complaints

15.1. Complaints and enquiries about the operation of the University's surveillance system should be sent to the University's Head of Campus Safety. Concerns about how data is being processed should be directed to the University's Data Protection Officer.

15.2. Where appropriate, allegations or complaints will be investigated under the University's normal grievance procedures.

15.3. Non-standard requests relating to the University's surveillance system will be handled centrally under the terms of the Freedom of Information Act, 2000.

16. Audit

16.1. The University will conduct periodic audits to assess compliance with this Policy.

Exceptions

17. There are no exceptions to this policy.

Monitoring and review

18. Overall responsibility for data protection in the University is delegated from the Vice Chancellor, via the Chief Financial and Operating Officer, as Senior Information Risk Owner, to the Data Protection Officer.

19. The Information Security Board, chaired by the Senior Information Risk Owner, is responsible for approval of data protection related policy.

20. This policy is updated as necessary and reviewed annually.

Document control

Approval body:	Information Security Board
Policy Owner:	Chief Financial and Operating Officer (CFOO)
Responsible Service:	Directorate of Technology, Estates and Facilities (DTEF)
Policy Manager:	Data Protection Officer

External regulatory and/or legal requirement addressed	UK General Data Protection Regulation, Data Protection Act 2018, Surveillance Camera Code of Practice, 2022.
Equality Impact Assessment	Not relevant for this policy.
Approval date:	v1 approved 23 March 2017. v1.1 approved 31 July 2019. v1.2 approved 22 May 2024. v1.3 approved 30 July 2025. v1.4 approved 18 November 2026.
Effective from:	18 November 2026
Date of next review:	November 2027