



CCTV POLICY

1. INTRODUCTION

- 1.1 York St John Students' Union (YSJSU) is committed to ensuring the welfare of all its employees and the security of its customers and employees. It has therefore introduced CCTV cameras to its building.
- 1.2 The purpose of the system is:
 - (a) to act as a deterrent to intruders;
 - (b) to assist in the prevention or investigation of crime or fraud;
 - (c) as evidence of any act that is the subject of an investigation and/or disciplinary or grievance hearing.
- 1.3 This policy applies to all YSJSU employees whatever their position.
- 1.4 Any inappropriate use of the CCTV cameras or film, whether under this policy or otherwise, may lead to disciplinary action being taken against employees under the Students' Union's disciplinary procedures. This may include summary dismissal.
- 1.5 The use of CCTV in the Students' Union does not reduce the necessity for employees to remain vigilant and report any suspicious or unlawful acts.
- 1.6 It is important that employees read this policy carefully. If there is anything that employees do not understand, they are advised to discuss it with their line manager.

2. POLICY STATEMENT

- 2.1 YSJSU trusts employees to use the CCTV cameras sensibly, professionally, lawfully, consistently with their duties, with respect for colleagues and the general public and in accordance with this policy and the Students' Union's rules and procedures.
- 2.2 YSJSU takes note of and endeavours to adhere to the [Home Office Surveillance Camera Code of Practice](#) dated June 2013.

3. GENERAL PRINCIPLES

- 3.1 The unlawful use of CCTV may result in the Students' Union being fined and may put at risk the welfare of employees and the security of systems.
- 3.2 Operators of the system should therefore exercise care when using the system. This includes the positioning of cameras and signs, the monitoring of images, the security of cameras, the storage of images, the disclosure of images and the rights of individuals in relation to CCTV.

4. USE OF THE CCTV SYSTEM

- 4.1 Operators of the system must be aware of the purpose for which each camera has been installed and any restrictions placed on employees concerning the use of the CCTV system.
- 4.2 Any adjustment by the operator of cameras must not be done so as to overlook spaces that are not intended to be covered.
- 4.3 Operators must not use the CCTV system in a way, which may damage, overload or affect its performance.

5. ACCESS TO RECORDED IMAGES

- 5.1 Access to recorded images is restricted to those persons who need to use the equipment and have the authority to access the images.
- 5.2 The following must be documented by any person who has access to the recorded images:
 - (a) the date and time at which access was allowed;
 - (b) the identification of any third party who was allowed access;
 - (c) the reasons for allowing access; and
 - (d) the extent of the information to which access was allowed.

6. VIEWING OF RECORDED IMAGES

- 6.1 Recorded images should only be viewed in an area designated for such viewing.
- 6.2 Access to this area is restricted to those persons who have been granted the authority to view the images.

7. REMOVAL OF CCTV IMAGES

- 7.1 If a tape or disk or other media containing recorded images is removed from the place where they are normally stored for the purpose of viewing, the following should be documented:
 - (a) the date and time of removal;
 - (b) the name of the person removing the tapes or images;
 - (c) the name of the person viewing the tapes or images including any third parties;
 - (d) the reason for removing the images;
 - (e) the outcome if any of the viewing; and
 - (f) the date and time that the tapes, disks or other media were returned to the place from which they were removed or, if not returned, whether the tapes, disks or other media were retained for evidential purposes.
- 7.2 If any media containing recorded images are removed for use in legal proceedings, the following must also be documented:
 - (a) any crime incident number to which the images may be relevant; and
 - (b) the location of media.

8. STORAGE

- 8.1 All recordings of CCTV images must be retained in a secure place to which access is controlled.

9. PASSWORD SECURITY

- 9.1 Under no circumstances should a user of the system disclose their password to a third party.

10. TRAINING

- 10.1 The Students' Union will provide training in the use of CCTV which employees must undertake if requested to do so.

11. DISCLOSURE OF CCTV IMAGES

- 11.1 No CCTV images should be disclosed unless the person to whom they are being disclosed to has the authority to receive them. In normal circumstances this will be the police and the person whose image has been processed on the system.

- 11.2 Operators should be aware of the disclosure procedures that have been implemented by the Students' Union.

- 11.3 Recorded images must not be routinely made available, for example to the media or on the internet. If images are made available in this way, the individuals must be disguised or blurred so that they are not readily identifiable.

- 11.4 If the CCTV system does not have the facility to edit, disguise or blur images in this way, an editing company or agent should be hired to perform this function. A written contract must be put in place between the Students' Union and the editing company or agent that includes the following:

- (a) all the tasks to be carried out by the editing company or agent;
- (b) that the editing company or agent is to act only on the instruction of the Students' Union;
- (c) the steps to be taken by the editing company or agent to ensure the reliability of his employees who have access to the images;
- (d) the technical and organisational security measures to be taken by the editing company or agent in regard to the images;
- (e) an obligation by the editing company or agent to allow the Students' Union to audit the editing company or agent's systems to ensure that the security of the images is protected.

12. DISCLOSURE TO DATA SUBJECTS

- 12.1 Individuals are entitled to access any recorded images of themselves on the CCTV system. Any individual making a request for such access should be provided with the following information:

- (a) the types of images recorded;

- (b) the purposes for which those images were recorded; and
- (c) any further information concerning the Students' Union's disclosure policy in respect of those images.

12.2 A subject access request form should also be provided. This should:

- (a) indicate any information required in order to locate the requested images;
- (b) indicate any information required to identify and verify the identity of the person making the request;
- (c) state the fee charged for carrying out this request, up to a maximum of £10; and
- (d) give the opportunity for the individual personally to view the recorded images.

12.3 The Students' Union will designate a member of staff from time to time to deal with subject access requests. All other employees of the Students' Union will receive instruction on how to recognise a subject access request and all such requests must be passed on to the designated member of staff.

12.4 If a recording is precluded from disclosure under a subject access request because the images of third parties are visible on the recording, the images of these third parties must be disguised or blurred. If the CCTV system does not have the facility to carry out such editing, a written contract should be made with an editing company or agent as described in paragraph 11.4 above.

12.5 If a subject access request cannot be complied with, the designated member of staff should document the identity of the person making the request, the date of the request and the reason for its denial. This record should be signed by the member of staff who has made the decision.

13. CESSATION OF MONITORING

13.1 As employees, employees have the right to ask the Students' Union to cease or not to begin CCTV monitoring in the workplace if it is causing or likely to cause substantial damage to them.

The Students' Union may amend this policy from time to time and an amended copy will be issued accordingly.