

September 2018

WGSU CCTV Policy

1. Introduction

This policy details the operating policy and standards for the surveillance system installed and operated by WGSU and THEM Ltd in compliance with the Data Protection Act 2018. This policy should be read in conjunction with WGSU's Privacy Policy which specifically sets out how the organisation will use information collected in relation to its members and staff.

2. Definitions

Throughout this policy, the following definitions will apply:

- 2.1. WGSU refers to Wrexham Glyndwr Students' Union (the Data Controller)
- 2.2. THEM Ltd is the company which operates the licenced premises 'The Lazy Lion' in the Union building
- 2.3. CCTV is the closed circuit television system in use in the WGSU premises
- 2.4. ICO is the Information Commissioner's Office

3. Ownership and Operation

The CCTV and all material are owned by WGSU who is registered with the ICO as a data controller. Operation of the CCTV will be by both WGSU and THEM Ltd.

4. The Purpose of the CCTV

The purpose of the CCTV systems in use at WGSU is broadly to enable to prevention, investigation and detection of crime and monitoring of the security and safety of the premises at WGSU. It is intended to ensure the maintenance of high standards of health and safety and for the review and investigation of accidents and incidents within the premises. It is also a condition of the Premises Licence (WXM/PREM/0255).

For these reasons, the information processes may include visual images, personal appearance and behaviours. This information may be about staff, contractors, customers and clients, suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance.

5. Principles

The following principles will govern the operation of the CCTV system:

- 5.1. Systems will be operated lawfully and only for the purposes set out in this policy and in accordance with the Data Protection Act.
- 5.2. To ensure compliance with the Data Protection Act, personal data, which includes biometric data recorded on all CCTV systems, will at all times be processed in line with GDPR principles. These principles require that data shall be:
 - 5.2.1. Processed lawfully, fairly and in a transparent manner
 - 5.2.2. Collected only for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
 - 5.2.3. Adequate, relevant and limited to what is necessary, in relation to the purposes of processing
 - 5.2.4. Accurate and kept up to date, where necessary, with all reasonable steps taken to ensure inaccurate data is rectified without delay
 - 5.2.5. Kept only for the period necessary for processing
 - 5.2.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and accidental loss, destruction or damage

6. System details

The CCTV system comprises of 4 visible cameras placed in various location of the WGSU premises (the Lazy Lion bar, building entrance, outside the toilet facilities and back office safe area). These CCTV cameras continuously record activities in these areas; visual only, no audio. The images are stored on a hard drive locally a restricted area and are only accessible by designated staff. Images can be viewed remotely by designated staff with password restricted access.

7. Operating standards

7.1. Cameras should not be hidden from view and signs will be prominently displayed at the point of entry to WGSU premises and at strategic locations where the system is operated. The signs will indicate:

- 7.1.1. That CCTV recording is taking place within these areas
- 7.1.2. The purpose for which CCTV is being captured
- 7.1.3. The contact details of the data controller

7.2. It is imperative that access to, and security of, images is managed in accordance with the requirements of the Data Protection Act. At all times the following standards will apply:

- 7.2.1. Surveillance recordings and other materials produced from them will not be retained for longer than necessary. Data storage is automatically managed by the CCTV digital records which uses software programmed to overwrite historical data in chronological order. This process produces an approximate 31 day rotation in data retention.
- 7.2.2. Provided that there is no legitimate or legal reason for retaining the CCTV images, the images will be erased following the expiration of the retention period of 31 days.
- 7.2.3. Where further investigation may be required, data will be retained beyond the retention period and will be stored in a secure place to which access is controlled.
- 7.2.4. The ability to view live and historical CCTV data is only provided at designated locations and to authorised persons only.
- 7.2.5. Except where a request has been granted for third party access to certain specified surveillance images, images are not to be displayed in the presence of any unauthorised person. For the purposes of viewing CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of WGSU or THEM Ltd who has operational responsibility for either the prevention, investigation and detection of crime and/or the monitoring of the security and safety of the premises.

8. Access to/disclosure of CCTV images

Requests for access to, or disclosure of images recorded on CCTV will only be granted if the request falls within the following:

- 8.1. Data subjects (i.e. persons whose images have been recorded by the CCTV)
- 8.2. Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- 8.3. Prosecution agencies

9. Data Subject Access Request

- 9.1. Data subjects have a right to make a data subject access request. To make a data subject access request, the individual should complete the form on the WGSU website. In some cases we may need to ask for proof of identification before the request can be processed.
- 9.2. If a subject access request is manifestly unfounded or excessive, WGSU is not obliged to comply with it. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

- 9.3. Where a data subject requests access to recordings believed to contain their personal data, the data set requested will be reviewed. Should the personal data of any other individual be contained within the data set request then access will not be permitted.
- 9.4. WGSU has the right to refuse Subject Access Request where such access could prejudice the prevention or detection of crime, the apprehension or prosecution of offenders or where multiple subjects are contained within the digital images who have not consented to their personal data being shared. If a Subject Access Request is refused, the reasons will be fully documented.

10. Request from a third party for access/disclosure

Authorities such as the police, government departments and local authorities with regulatory powers are able to request access to personal data without the consent of the data subject for the purposes of:

- 10.1. The prevention and detection of crime
- 10.2. The apprehension or prosecution of offenders
- 10.3. The assessment or collection of tax or duty

This does not give an automatic right to access the information. Any request for disclosure should be submitted in writing to the WGSU CEO and/or THEM Ltd MD for review and decision regarding the appropriateness of releasing of data.