Policy Title:	Surveillance Systems Policy
Audience:	Public
Policy Date:	March 2018

1. Introduction

This policy details the operating policy and standards for the surveillance systems installed and operated by RHSU in compliance with General Data Protection Regulations (GDPR). This includes CCTV, Body Worn Video and Dash Cams.

The policy sets out the purpose and principles of data management and the operating standards of the systems.

The processing of personal data (i.e. the collection, use and storage of personal data) must comply with General Data Protection Regulations 2016 (GDPR). For this reason this policy should be read in conjunction with the organisation's GDPR Policy and the Privacy Policy, which specifically sets out how the organisation will use information collected in relation to its staff and members.

2. Definitions

Throughout this policy the following definitions will apply:

- RHSU refers to the organisation known as Royal Holloway Students' Union (the Data Controller)
- CCTV is the closed circuit television system in use in all RHSU premises
- BWV is the body worn CCTV system in use by designated licensed security personnel employed by RHSU
- Dash Cam is the vehicle mounted CCTV system in use on the RHSU Union Bus service.
- ICO is the Information Commissioner's Office

3. Ownership and operation

The CCTV, BWV and Dash Cam systems and all recorded material and copyright are owned by RHSU. RHSU is registered with the ICO as a Data Controller operating closed circuit surveillance systems.

4. Purpose of the CCTV, BWV and Dash Cam systems

The purpose of the CCTV systems in use at RHSU is broadly to enable the prevention, investigation and detection of crime and monitoring of the security and safety of the premises at RHSU.

Specifically, the system is intended to be used for:

- Maintaining the security of property and premises and for preventing and investigating crime
- Maintaining high standards of health and safety and for the review and investigation of accidents and incidents within the premises
- Delivery of the four licensing objectives as defined within the Licensing Act 2003
    - Prevention of crime and disorder
    - Public safety
    - Prevention of public nuisance
    - Protection of children from harm
- Insurance compliance and incident investigation

For these reasons the information processed 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 CCTV, BMW and Dash Cam systems:

i. Systems will be operated lawfully and only for the purposes set out in this policy and in accordance with the ICO Data Protection Register.

ii. To ensure compliance with GDPR, personal data, which includes biometric data recorded on all CCTV systems, will at all times be processed in the line with the GDPR principles. These principles require that data shall be:

   a. Processed lawfully, fairly and in a transparent manner
   b. Collected only for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
   c. Adequate, relevant and limited to what is necessary in relation to the purposes of processing
   d. Accurate and kept up to date, where necessary, with all reasonable steps taken to ensure that inaccurate data is rectified without delay
   e. Kept only for the period necessary for processing
   f. 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

6.1 The CCTV system comprises of both visible and discreet cameras situated in various locations around RHSU premises, which continuously record activities in these areas. The images are stored in network video recorders secured locally in restricted areas and are only accessible by delegated staff with password controlled access.

6.2 The BWV system comprises of visible cameras attached to key personnel in the employment of RHSU, which record activities when activated by the person. This system works in partnership with the CCTV system to continuously record activities during defined licensed operating hours.

6.3 The Dash Cam system comprises of visible cameras attached to the windscreen of the minibuses operated by RHSU, and continuously record activities in and around these vehicles when operated by RHSU as the Union Bus Service. The cameras are not installed in the vehicles for any other activity.

6.4 The images for both BWV and Dash Cam are stored on an encrypted hard drive and secured centrally in the RHSU Finance office and are only accessible by delegated staff with password controlled access.

7. Operating standards

7.1 <u>Installation and signage</u>

Cameras shall not be hidden from view and signs will be prominently displayed at the point of entry to all RHSU premises and property, and at strategic locations, where surveillance systems are operated. Employees operating BWV will be defined within the premises event management procedures and will be wearing signs informing individuals that cameras are in operation. The signs will indicate:

- That CCTV recording is taking place within these areas
- The purpose for which CCTV is being captured
- The contact details of the Data Controller

7.2 Processing CCTV images

It is imperative that access to, and security of, images is managed in accordance with the requirements of GDPR. 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.

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. Data will be erased when the purposes for processing have been met. For guidance purposes this would usually be in accordance with the following:

- Maintaining the security of property and premises and for preventing and investigating crime – 3 months
- Maintaining high standards of health and safety and for the review and investigation of accidents and incidents within the premises – 3 months
- Insurance compliance and incident investigation – 3 years

7.2.4 The ability to view live and historical CCTV data is only to be 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 (see below), 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 RHSU 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 at RHSU.

7.3 Covert Recordings

Covert cameras may be used within pre-defined CCTV areas under the following circumstances on the authorisation of the senior management team, following the completion of a Privacy Impact Assessment:

- That informing the individual(s) concerned that recording is taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the data protection principles and lawful processing requirements and will only relate to the specific suspected unauthorised or illegal activity. The decision to adopt covert recording will be fully documented in the Privacy Impact Assessment.

8. Access to/disclosure of CCTV images

8.1 Requests for access to, or disclosure of, images recorded on surveillance systems will only be granted if the requestor falls within the following:

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

8.2 Data Subject Access Request

Data subjects have a right to make a data subject access request. To make a data subject access request, the individual should submit an email request to helpdesk@su.rhul.ac.uk In some cases we may need to ask for proof of identification before the request can be processed.

8.2.1 The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where large amounts of the individual's data is being processed, it may respond within three months of the date the request is received. RHSU will write to the individual within one month of receiving the original request to tell them if this is the case.

8.2.2 If a subject access request is manifestly unfounded or excessive, RHSU is not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. 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.

8.2.3 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 for any other individual be contained within the data set requested then access will not be permitted.

8.2.4 RHSU has the right to refuse a 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.

8.3 Request from a third party for access / disclosure

8.3.1 Under section 29 of the Data Protection Act 1998 ‘relevant authorities’ such as the police, government departments and local authorities with the regulatory powers are able to request access to personal data without the consent of the data subject for the purposes of:

- The prevention or detection of crime
- The apprehension or prosecution of offenders
- The assessment or collection of tax or duty

Section 29 of the Act does not give an automatic right of access to information. The Act states that public bodies can assess the merits of requests and decide whether or not to apply section 29.

8.3.2 Any request for disclosure by the Police should be made using the Information Disclosure Request Form. This should be submitted to senior management for review and decision regarding the appropriateness of releasing data.