Surveillance Systems Policy

From: Chief Information Officer **Date:** April 2018

1 Relevant law

1.1 The General Data Protection Regulation (GDPR) will be incorporated into UK law via the Data Protection Act 2018. These are referred to in this policy as the Data Protection Legislation as defined in the **Glossary of Terms**.

1.2 See also the **Surveillance Camera Code of Practice** issued under the Protection of Freedoms Act 2012 and the Information Commissioner's **CCTV Code of Practice**.

1.3 The definition of **Surveillance Systems** and other terms used in this policy are set out in **Schedule 1**.

2 Introduction

2.1 Surveillance Systems collect and record **Personal Data** and potentially **Special Category Data**. This Policy describes how University Surveillance Systems are to be used so that compliance with the Data Protection Legislation and associated guidance and regulations is assured.

2.2 It replaces the existing CCTV Code of Practice and includes systems that are in use, in the process of being introduced or are likely to be considered for use in the foreseeable future.

3 Scope

3.1 This policy applies to University of Southampton staff, students, agency staff, visitors, contractors and third parties (Users).

3.2 This policy is written in the context of the Data Protection Legislation as it pertains to an individual's right to privacy and not to cover any Health and Safety risks, which will be addressed through specific procedures and risk assessments.

4 Aims

4.1 This policy's aim is to lay down the guidelines for the use of Surveillance Systems and Personal Data obtained from them in compliance with the Data Protection Legislation.

5 Data Protection Principles

5.1 The Data Protection Legislation contains a number of principles that govern the processing of Personal Data. The principles are set out in **Schedule 2**.

6 Roles and Responsibilities

6.1 The Chief Operating Officer has responsibility for managing information risks that may impact on the strategic business goals of the University and has responsibility for reporting to the University's governing body via the Audit Committee.

6.2 The Chief Information Officer is the Senior Information Risk Owner (SIRO) and has responsibility for ensuring compliance with this policy and for maintaining the currency of this policy.

6.3 The Chief Security Officer, in consultation with the Data Protection Officer, has responsibility for ensuring that training is provided for Authorised Users, where appropriate, to further their understanding of the of the principles of the Data Protection Legislation and their application.

6.4 The Chief Security Officer or, in their absence, their deputy has responsibility for the management of Surveillance Systems and for:

6.4.1 Selecting camera sites and initial areas to be viewed;

6.4.2 Being responsible for compliance with the Data Protection Legislation;

6.4.3 Taking responsibility for control of the Recorded Material and make decisions on how these can be used in conjunction with senior management;

6.4.4 Ensuring that data obtained through the use of CCTV and BWV Surveillance Systems is secure and only viewed by Authorised Users;

6.4.5 Ensuring that the procedures complimenting this Policy comply with the guidance produced by the Information Commissioner's Office, the Surveillance Camera Commissioner and by the Home Office;

6.4.6 Introducing a CCTV incident log and record of Police or other Statutory Authority requests for Recorded Material;

6.4.7 Making bi-annual checks to establish that nominated managers still require viewing rights of the system in line with the above objectives;

6.4.8 Ensuring adequate signage is erected in line with the Information Commissioner's **Code of Practice**;

6.4.9 Regularly evaluating the system to ensure it complies with the latest legislation, CCTV Codes of Practice and its use is in accordance with this policy.

6.5 The Deputy Chief Security Officer is responsible for day to day administration of Surveillance Systems and for:

6.5.1 Clearly communicating the specific purposes of the recording of and use of the Recorded Material and objectives to all security staff;

6.5.2 Ensuring that a Surveillance Systems incident log and record of Police or other Statutory Authority requests for Recorded Material is maintained. This document will be readily available and held in the Central Control Room;

6.5.3 Carrying out annual review to check that procedures are being complied with;

6.5.4 Ensuring that the audit team includes Surveillance Systems practices and procedures on their regular audits of the University's Security Services;

6.5.5 Ensuring that Recorded Material archived for investigatory reasons are deleted after three months;

6.5.6 Ensuring that all Data Protection Legislation forms received from the Police or other investigatory bodies e.g. Health and Safety Executive are copied to the Data Protection Officer and are filed for future reference;

6.5.7 Ensuring that all Recorded Material are automatically erased after a period of one (1) month unless retained for evidential purposes.

6.6 Authorised Users will be responsible for:

6.6.1 Selecting the appropriate Personal Data to be recorded on controllable cameras (PTZ) as Defined in Schedule 1 (1) (d) (ii) so as to comply with the objectives outlined above;

6.6.2 Ensuring that the targeting of individuals with Surveillance Systems is only conducted when there is reasonable suspicion that the person falls within one of the objectives set above e.g. committing a criminal offence.

6.7 The Data Protection Officer is responsible for informing and advising the University on its obligations under the Data Protection Legislation and will include the Surveillance System on the University's data protection notification to the Information Commissioners Office.

6.8 All Authorised Users involved in operating the Surveillance Systems are expected to have read this policy prior to being instructed on the operation of the system and ensure that they understand and apply the principles of the Data Protection Legislation and comply with the best practice guidelines set out in **Schedule 3**.

7 Best Practice Guidelines for Use of Surveillance Systems & BWV

7.1 Guidelines as to the use of Surveillance Systems and BWV including the storing, viewing and disclosure of Recorded Material are set out in **Schedule 3**.

8 Data Subject rights and privacy contacts.

8.1 The Data Protection Legislation gives the Data Subject rights in respect of the Personal Data held about them by the University. These rights are set out in **Schedule 4**.

8.2 The University has introduced a **ServiceNow** platform to manage Data Subject requests for Personal Data to assist the University in meeting its timeliness and compliance obligations under the Data Protection Legislation.

8.3 Data Subject requests for access, rectification, erasure, portability and objections as to processing, to/of their Personal Data should be made through the University's website. Data Subject who are members of the University and have a University login and email account may submit their request via their University email account to: **data.protection@soton.ac.uk**.

8.4 All other requesters must upload and submit any supporting documentation verifying that they are the Data Subject or acting on behalf of the Data Subject through **Servicenow**. See Schedule 4 for a list of Data Subject rights.

8.5 For general enquiries about the University's Data Protection Policy and the Data Protection Legislation please contact:

The Data Protection Officer
Legal Services,
University of Southampton, Highfield, Southampton S017 1BJ
Telephone: (023) 8059 2400, e-mail: data.protection@soton.ac.uk

8.6 A log of such request will be maintained in the Central Control Room disclosure log.

9 Freedom of Information

9.1 Please refer to the University's Freedom of Information Policy.

10 Intellectual Property

10.1 All Recorded Material and any other recordings produced by the surveillance systems remain the property and copyright of the University.

11 Disciplinary Offences

11.1 Unlawful obtaining or disclosure of personal data (including the transfer of personal data outside the EEA) or any other breach of the Data Protection Legislation by Authorised Users will be treated seriously by the University and may lead to disciplinary action up to and including dismissal or expulsion and must be reported.

11.2 The University will only investigate data obtained by the surveillance systems in a staff disciplinary case when there is a suspicion of misconduct and not to generally monitor staff activity. Investigating managers must seek advice from an HR Advisor before requesting CCTV imagery. In these situations, the HR Advisor will formally request access to the Recorded Material from the Chief Information Officer and the Data Protection Officer. If approval is given, Security Services will provide the Recorded Material where these may assist the investigation into misconduct. Where access is given, the confidentiality of the Recorded Material and who is able to access them will be closely controlled.

11.3 The University will only investigate data obtained by the surveillance systems as evidence in a serious student disciplinary case when there is a suspicion of misconduct and not to generally monitor student activity. Investigating managers must seek formal approval from the Chief Information Officer and the Data Protection Officer before requesting CCTV imagery. If approval is given, Security Services will provide the Recorded Material where these may assist the investigation into misconduct. Where access is given, the confidentiality of the Recorded Material and who is able to access them will be closely controlled.

12 Complaints

12.1 Complaints received in relation to the use of the Surveillance Systems are to be made to the Chief Security Officer who will investigate the complaint in accordance with the appropriate University complaints procedure. If necessary, the complaint will be escalated to the Chief Information Officer and the Data Protection Officer, where appropriate, for further action/review.

12.2 Complaints in relation to the disclosure or image supply are to be made in writing to the Chief Security Officer who will investigate the complaint and, if necessary, the complaint will be escalated to the Chief Information Officer and the Data Protection Officer, where appropriate, for further action/review.

12.3 If the complaint is in respect of a personal data breach Authorised Users must follow the processes set out in the University's **Data Breach Guidelines.**

12.4 Serious breaches must be reported to the Data Protection Officer immediately on discovery and no later than 24 hours after the breach has occurred by emailing: **databreach@soton.ac.uk** or contacting the Data Protection Officer as above.

12.5 A record of any personal data breaches will be kept by the Data Protection Officer.

13 Monitoring compliance and review

13.1 All University policies and procedures will be subject to periodic audit and review to ensure that they remain fit for purpose and the University remain compliant.

14 Further information

14.1 Please see the University's Data Protection Policy and additional policies and guidelines concerning particular activities at our **Publication Scheme**.

Document Control

File Name	Surveillance Policy
Original Author(s)	Nick Povey
Current Revision Author(s)	Legal Services
Owner	Chief information Officer
Publication Date	
Target Audience	

Version History

Version	Date	Author(s)	Notes on Revisions
00.01	May 2018		

Document Sign Off

Name	Role	Doc version	Signoff date	Signature*
Barbara Halliday	Director of Legal Services	1	24-05-2018	
Professor Simon Cox	Chief Information Officer	1	24-05-2018	

*If signoffs are received by email, print names here and archive the sign off emails. Add location of signoff emails here:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.

Schedule 1 **Definitions**

1 The following definitions apply to this policy:

1.1 **Authorised User**: security staff, the CCTV Maintenance Team, management staff with a legitimate reason for accessing the Recorded Material – e.g. managers / HR investigating the potential misconduct of staff, bars managers to monitor legal compliance, laboratory superintendents to monitor safety and Halls staff to monitor anti-social behaviour, police Officers, other Statutory Officers e.g. Health and Safety Executive Officers, University Health and Safety Advisers/Management, members of staff facing disciplinary action and Trade Union officials representing them and students facing disciplinary action and their representatives.

1.2 **Data Protection Legislation**: (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 1998 ("**DPA**") and EC Directive 95/46/EC (the "**DP Directive**") (up to and including 24 May 2018) and on and from 25 May 2018, the GDPR and all legislation enacted in the UK in respect of the protection of personal data; and (b) any code of practice or guidance published by the ICO (or equivalent regulatory body) from time to time;

1.3 **Personal data**: any information that can identify an individual either on its own or in combination with other information and can include photographs and video footage collected and recorded by Surveillance Systems.

1.4 **Recorded material**: Personal Data collected and recorded by Surveillance Systems.

1.5 **Special Category Data**: Personal Data consisting of information relating to the data subject with regard to racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, physical or mental health or condition, sexual life, the commission/alleged commission of an offence alleged/committed by the data subject and any related court proceedings, trade union membership. It also includes genetic and biometric data where processed to uniquely identify an individual.

1.6 **Surveillance Systems**:

1.6.1 Automatic Number Plate Recognition (ANPR): means a technology that uses cameras to read vehicle registration plates linked to a secure computerised system, it can be

linked to the DVLA and Police databases to prevent and detect crime or by local system owners on private land to monitor and manage vehicles.

1.6.2 Body worn video (BWV) means video cameras worn by an individual normally overtly that are capable of recording images and sound. The cameras will only be activated by the wearer when managing an incident that is likely to be subject to review or investigation. BWV can capture Personal Data and potentially Special Catagory Data.

1.6.3 Closed Circuit Television (CCTV): means a television system in which signals are not publicly distributed but are monitored, primarily for safety and security purposes. The system is made up of strategically placed cameras linked via a secure IT network to video recorder(s) and with images monitored elsewhere from a controlled environment. The system records images but not sound. CCTV Cameras cover roadways, car parks, buildings, vulnerable public facing offices, academic buildings and licensed premises. Images are recorded locally within departments or centrally on network video recorders and monitored by Central Control Room staff. In addition, a limited number of management staff have the facility to monitor cameras cited within their own areas of responsibility i.e. to monitor legal compliance (bars managers), safety (laboratory superintendents) and anti-social behaviour (Resident Support Staff (RSA's)). There are several types of CCTV camera:

(i) Overt fixed – these record uncontrolled images e.g. reception desk, doors etc.

(ii) Overt Pan, Tilt and Zoom (PTZ) – these are controllable cameras that can follow vehicles or subjects when required.

(iii) Covert cameras – temporary fitted cameras used in areas not covered by CCTV but the scene of persistent criminality.

(iv) Overt PTZ High Definition (HD) cameras – these are controllable cameras that can follow vehicles or subjects when required and are placed in incident hotspots, e.g. Bus Interchange, to record images that can be interrogated in detail after the event, e.g. zoomed into for identification purposes.

(v) ANPR – these record vehicle number plates together with a date and time stamp.

1.6.4 Covert Surveillance: means an observation of a location or person in a way that tries to ensure the subject is unaware it is, or could be, taking place. The surveillance may be undertaken by a person or through the use of a recording device. Authorisation by the Chief Operating Officer or their delegated deputy is required before covert surveillance can be undertaken. The installed systems will be reviewed every 31 days with the appropriate permissions being sought to continue with the

operation. The systems will be removed as soon as practicably possible after the operation has ceased.

1.6.5 Unmanned Aerial Vehicles (UAVs) or Drones: means an unmanned aircraft (helicopter or fixed wing) that fly either autonomously or by person operated radio control. In most circumstances the UAV carries a camera to obtain images or provide surveillance. Please refer to the University's Health and Safety UAV Policy.

1.6.6 Any other systems that capture information of identifiable individuals or information relating to individuals.

Schedule 2 **Data Protection Principles**

2 Principles

2.1 The following principles apply when processing personal data. The term "processing" applies to all operations performed on the personal data during its life cycle including collection, storage, use and destruction. Personal data shall be:

2.1.1 Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

2.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (purpose limitation).

2.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

2.1.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

2.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (storage limitation).

2.1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

The Data Controller shall be responsible for, and be able to demonstrate compliance with, the above principles (accountability).

Schedule 3 **Best Practice Guidelines**

3 Use of Surveillance Systems

3.1 Introduction

3.1.1 A Data Protection Impact Assessment must be carried out before a Surveillance System is implemented. It shall include consideration of the pressing need that the Surveillance System is intended to address and whether its proposed use has a lawful basis and is justified, necessary and proportionate.

3.1.2 Existing Surveillance Systems should be the subject of an annual evaluation to ensure that it is necessary and proportionate to continue to use it.

3.1.3 Surveillance Systems can be used to observe the Campus and areas under surveillance and identify incidents that require a response; the response must be proportionate to the incident being witnessed. On some occasions, the deployment of a security officer may be sufficient; on other occasions, contacting the Police to respond may be the appropriate action.

3.1.4 Such surveillance is to be in accordance with the stipulated objectives set out below in Clauses 3.2, 3.3 and 3.4.

3.1.5 Whenever a response is required, a log must be completed on the incident reporting system.

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

3.2 Objectives for the use of Surveillance Systems are to:

3.2.1 Assist in providing a safe and secure environment for the benefit of those who might visit, work or live on the campus;

3.2.2 Reduce crime and the fear of crime by reassuring students, staff and visitors whilst acting as a deterrent against crime, public disorder and anti-social behaviour;

3.2.3 Assist the police to Identify, apprehend and prosecute offenders in relation to crime, public disorder and anti-social behaviour;

3.2.4 Provide the Police, Health and Safety Executive and University with evidence upon which to take criminal, civil and disciplinary action respectively;

3.2.5 Monitor and assist with crowd management during University events;

3.2.6 Monitor and assist with traffic management;

3.2.7 Assist in the monitoring and deployment of security staff during normal duties and emergency situations;

3.2.8 Act as a deterrent to violence and threats against security officers;

3.2.9 Obtain evidence for use in the investigation of criminal actions, breaches of health and safety legislation and breaches of student and staff disciplinary procedures.

3.3 Specific objectives for the use of UAVs' (Drones): (See separate UAV Policy)

3.3.1 Any personal data incidentally obtained with the use of Drones will be managed by the Drone user in accordance with the Data Protection Legislation.

3.4 Covert cameras or human surveillance

Covert cameras or human surveillance will be used only when a series of criminal acts have taken place e.g. thefts in the same area or where there is a suspicion of serious misconduct. Authority from the University's Chief Operating Officer or their nominee will always be sought before installing any covert cameras or undertaking human surveillance. It is to be noted that provided that authority has been sought and given prior to usage, in line with this procedure, then recording will not constitute misconduct and will be usable in any subsequent disciplinary or criminal proceedings

3.4.1 These objectives will be closely followed when assessing the requirements for new or continued surveillance. If designated usage of an area changes, it will be necessary to assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

3.5 Objectives for the use of Body Worn Video (BWV)

3.5.1 BWVs will be used overtly by uniformed Security Officers who have been trained in the function of the device, circumstances where it can be used and on their and the University's responsibility's under the Data Protection Legislation. It is the BWV user who decides if and when the device is used and who will announce when the device is turned on and off. Whilst recording, the Recorded Material are displayed on the devices screen visible to the subject.

3.5.2 The BWV user cannot delete or manipulate recordings. At the end of duty the BWV will be placed into its docking station and any Recorded Material will automatically download using encrypted and secure software, recordings will be marked as either evidential (in which case it will be stored for as long as required, subject to periodical review) and non-evidential (these recordings will be automatically deleted after 31 days). Once securely downloaded the recording on the BWV is automatically wiped and the device recharged ready for its next use.

3.5.3 Access to the Recorded Material is restricted to Security supervisors and managers and will be managed as for those collected via CCTV.

3.6 Signage

3.6.1 Signage should be clearly visible and readable. It should include the details of the University as the systems operator, a contact number for Security if there are any queries and the purpose of its use. The University has erected signage at the main entrances to the University Campus and at other locations where CCTV is in use, informing all that CCTV surveillance is in operation.

3.6.2 Signs should be an appropriate size in relation to its context.

3.6.3 Care must be taken when positioning CCTV cameras. Although the cameras may be positioned on site, they may still capture Recorded Material of people walking by. If this is the case, CCTV signage should be made visible outside the University environs as well.

3.7 Storing and Viewing Recorded Material

3.7.1 Recorded material should be stored in a way that maintains the integrity and security of the information and, where necessary, encrypted.

3.7.2 All Recorded Material on the University CCTV and BWV systems should be digitally stored on network video recorders that are accessible by Central Control Room staff or remotely within Departments, on computer/server hard drives so it is not possible to tamper with or alter the Recorded Material.

3.7.3 In the event of law enforcement agencies requiring the Recorded Material, the Recorded Material can be 'burnt' onto a CD/DVD for evidence in court, on receipt of the appropriate Data Protection Request form.

3.7.4 Recorded Material held for up to 31 days before they are automatically erased, however if required, Recorded Material can be 'locked' on the hard drive for future reference.

3.7.5 All other Recorded Material will be erased after 3 months unless required for evidential purposes in a court of law.

3.7.6 Locked Recorded Material are reviewed on a three (3) monthly basis and any not still required for evidential purposes will be deleted.

3.7.7 Recorded Material is generally viewed confidentially in secure private offices, however, they may also be viewed discreetly at authorised Security Managers' desks. Standard Operating Procedures regarding the viewing of recorded material are held by Security Management and should be adhered to at all times.

3.7.8 Third party requests to view Recorded Material are to be made in writing to the Deputy Chief Security Officer.

3.8 Disclosure

The following guidelines will be adhered to in relation to disclosure of Recorded Material:

3.8.1 Disclosure of Recorded material from Surveillance Systems must be controlled and consistent with the purpose(s) for which the system was established.

3.8.2 Any disclosure will be in line with the objectives set out in this Schedule.

3.8.3 Any requests for Recorded Material are to be made to the Chief Security Officer or his/her Deputy. In some limited circumstances, it may be appropriate to release Recorded Material to a third party, where their needs outweigh those of the individuals whose material is recorded. Please seek advice from the Chief Security Officer, his/her Deputy or from the Chief Information Officer and/or the Data Protection Officer, Legal Services.

3.8.4 Any disclosure will be controlled under the supervision of the Chief Security Officer or his/her deputy.

3.8.5 Any requests for the disclosure of Recorded Material by members of the general public or third parties (without a legal obligation to do so) must be agreed by Legal Services, the Chief Information Officer (as SIRO) and/or the Chief Operating Officer prior to release.

3.8.6 A log book/sheet will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for the disclosure.

3.8.7 The appropriate disclosure documentation from the Police will be filed for future reference.

3.8.8 Recorded Material will not be forwarded to the media for entertainment purposes or be placed on the internet.

3.8.9 Recorded Material will not be copied in any way, e.g. photographed, downloaded or printed for use other than described in the objectives.

3.8.10 Recorded Material will only be released to the media for identification purposes in liaison with the Police or other law enforcement agency.

3.8.11 The method of disclosing Recorded Material is to be secure to ensure that it is only seen by the intended recipient.

3.8.12 The obscuring of the Recorded Material of third parties not relevant to the investigation to prevent unnecessary identification of individuals will always be considered.

3.9 Security Central Control Room

3.9.1 The Security Central Control Room (CCR) is situated on level 1 of B32 and is capable of receiving Recorded Material from CCTV cameras throughout the University's campuses. It is staffed 24 hours a day by uniformed University Security Officers.

3.9.2 The Control Room is also equipped with a licensed radio system linking the Room with uniformed Security Officers who provide mobile and foot patrols of the institution and are able to respond to incidents identified on the Surveillance Systems.

Schedule 4 **Data Subject Rights**

4 Data Subject rights

4.1 The Data Protection Legislation enshrines the rights for Data subjects including the rights to:

4.1.1 Request access to data;

4.1.2 Prevent the processing of data for direct-marketing purposes (including profiling) and in certain other circumstances;

4.1.3 Ask to have inaccurate data amended;

4.1.4 Request a restriction to the processing of data in certain circumstances, including to stop processing data where the data subject believes it is likely to cause unwarranted substantial damage or distress to the data subject or someone else;

4.1.5 Request reconsideration of any solely automated decisions made that significant affects the data subject (where such decision-making is legally permissible);

4.1.6 Request that data be provided in a portable (structured, commonly used and machine-readable) format in certain circumstances.

4.1.7 Request the erasure of data.