UCL CCTV Policy

University College London

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

Document Summary

Document ID	TBD
Status	Approved
Information Classification	Restricted
Document Version	0.6

1 Policy owner

This policy is owned by the UCL SIRO.

2 Policy Contact

If you have any questions, comments or concerns regarding this policy, please contact the UCL Security Manager in the first instance.

3 History

Date	Version	Author	Approved by	Comments	
05.04.2018	0.5	Lee Shailer		Carried out a full review of the existing policy	
10.04.2018	0.5a	Ravi Miranda		Applied UCISA template, formatting, edits	
11.04.2018	0.5b	Lee Shailer		Further comments	
11.04.2018	0.5c	Lee Shailer, Paul Lamb, Ravi Miranda, Trevor Peacock		Edited document to provide clarity	
12.04.2018	0.5d	Paul Lamb, Ravi Miranda		Minor edits and corrections, improved Section 4, Added Section 15	
16.04.2018	0.5e	Lee Shailer, Ravi Miranda		Edited to accept 2 changes	
20.04.2018	0.5f	Ravi Miranda		Minor edits based on SWG Minutes	
27.04.2018	0.5g	Ravi Miranda, Trevor Peacock, Paul Lamb, Lee Shailer		Minor review based on SWG Minutes	
09.05.2018	0.5h	Lee Shailer, Ravi Miranda		Edited Definitions, About this Policy sections Inserted text for Policy Contact	
21.05.2018	0.6	Paul Lamb		Noted SWG's endorsement	

4 Review plan

The policy shall be reviewed every year to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards. A review may also be needed following changes in the above or in response to events, incidents or new risks.

5 Definitions

See Glossary. ***https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Glossary***

CCTV: means any surveillance system designed to capture and record images of individuals, or information relating to individuals, and property. The term includes CCTV as understood as a system of fixed cameras, but also covers any such technology including automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture personal data.

(The remainder of this section will be moved to the Glossary when the policy is published.)

PIA: A Privacy Impact Assessment is intended to assist in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether any limitations should be placed on their use.

Data: means information which is stored electronically. In respect of CCTV, this can mean video images. For the avoidance of doubt, screen shots of video images that have been printed out will fall within scope of Data Protection Legislation.

Data Protection Legislation: means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction which relates to the protection of individuals with regards to the Processing of Personal Data including the GDPR (from and including 25 May 2018) and/or (c) in the event that the UK leaves the European Union, all legislation enacted in the UK in respect of the protection of Personal Data.

6 Introduction

Surveillance Camera Systems also known as "CCTV" has a legitimate role to play in helping to maintain a safe and secure environment for all UCL's staff, students and visitors. However, this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns.

Images recorded by CCTV systems are personal data which must be processed in accordance with data protection laws and UCL's data protection policy. This policy is designed to help UCL comply with its legal obligations.

This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of data generated by CCTV could constitute a criminal offence.

7 About this Policy

UCL currently uses CCTV cameras to view and record individuals on and around its premises. This policy outlines the use of CCTV and the processing of data recorded by CCTV cameras to ensure that UCL is compliant with data protection law and best practise.

UCL recognises that images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the Data Protection Legislation. UCL is the data controller.

UCL uses CCTV around its site for the following legitimate business purposes:

a) to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
b) for the personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime;
c) to support law enforcement bodies in the prevention, detection and prosecution of crime;
d) to assist in day-to-day management, including ensuring the health and safety of staff and others;
e) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;
f) to assist in the defence of any civil litigation, including employment tribunal proceedings;
g) to assist with traffic management issues; and
h) to monitor the security of buildings.

8 Scope

The policy applies to all staff, contractors and students of UCL and all other persons authorized by UCL.

Any CCTV operated by or on behalf of UCL will fall within scope of this policy. Visitors and other members of the public may be captured by CCTV.

9 Dependencies

9.1 Documents which rely upon this policy:

Guidance on use of CCTV systems [to follow]

9.2 Documents which this policy relies on:

- UCL Information Security Policy
- UCL Computing Regulations (Acceptable Use Policy)
- UCL Data Protection Policy
- UCL Monitoring Computer and Network Use Policy
- UCL Policy on Connecting Equipment to the UCL Network
- UCL Records Retention Schedule
- UCL Information Management Policy

10 Related requirements

None applicable

11 Stakeholders

The following roles, or their nominated representatives, should be involved in the review of this document

- Policy Owner
- Security Manager
- Head of Information Security
- Data Protection Officer
- Chair of Security Working Group

12 Accountable Roles

As Data Custodian, the Security Manager has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy.

The Security Manager is responsible for the approval and running of CCTV systems on all UCL premises.

The Security Manager has responsibility for day-to-day management and operation of the central CCTV system, including specification, approval, operational aspects of the system and the storage of data recorded.

All staff who operate, manage or process images from CCTV shall observe this policy.

13 Policy statements

13.1 CCTV Operation

PS1 CCTV systems may operate 24 hours a day.

PS2 CCTV camera locations shall be chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV cameras shall not focus on private homes, gardens or other areas of private property.

PS3 CCTV camera systems shall not be configured to record sound unless a Privacy Impact Assessment has been completed and approval is given by the Data Protection Officer.

PS4 Authorised UCL staff may use body worn cameras in response to specific events.

PS5 Staff shall not use CCTV systems until they have completed appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

PS6 The Security Manager shall approve all existing and new use of CCTV.

PS7 Where CCTV cameras are placed in the workplace, UCL will ensure that adequate signs are displayed to alert individuals that their image may be recorded.

PS8 Authorised staff shall monitor live feeds from CCTV cameras where it is deemed reasonably necessary, for example to protect health and safety.

PS9 Recorded images shall be viewed by authorised members of staff. Recorded images shall only be viewed in designated, secure offices.

13.2 Use of Data gathered by CCTV

PS10 Data gathered from CCTV cameras shall be transmitted and stored in a way that maintains its integrity, availability and confidentiality, in order to ensure that the rights of individuals whose images recorded by the CCTV systems are protected.

PS11 Data shall be protected by appropriate technical measures e.g. encryption.

PS12 Contractual safeguards shall be in place to protect the security, confidentiality and integrity of relevant CCTV data, where data processors have been engaged.

13.3 Retention of CCTV images

PS13 Images will normally be retained for 18 days, but can be held for longer in the following circumstances:

a) Where compliance with a legal obligation requires an extended retention period; or
b) In specific circumstances in which longer retention periods are required to establish patterns of behaviour or to retain evidence and where the Data Protection Officer has authorised this; or
c) In the event that extended closure makes a longer retention period necessary and where the Data Protection Officer has authorised this.

PS14 Data and images recorded by the CCTV system shall be permanently and securely deleted once the purpose for which they were collected has expired. The Security

Manager shall maintain a log of when data are deleted.

PS15 Any physical matter such as tapes, discs, hard copy prints, still photographs shall be disposed of as confidential waste.

13.4 Additional Surveillance Camera Systems

PS16 A Privacy Impact Assessment (PIA) shall be carried out prior to introducing a new surveillance camera system or placing a new CCTV camera in a workplace location.

PS17 CCTV cameras shall only be placed in areas where there is an expectation of privacy (for example, in changing rooms) in very exceptional circumstances, i.e. where it is judged to be strictly necessary to deal with the most serious concerns or dangerous circumstances. Signage will be used where necessary.

13.5 Covert CCTV Monitoring

PS18 UCL will only engage in covert CCTV monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, UCL reasonably believes there is no less intrusive way to tackle the issue.

PS19 In the exceptional event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Security Manager and the Data Protection Officer.

PS20 Covert monitoring shall only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and shall only relate to the specific suspected illegal or unauthorised activity.

13.6 Review of CCTV use

PS21 The ongoing use of existing CCTV cameras in the workplace shall be reviewed regularly to ensure that their use remains necessary and appropriate, and that any surveillance camera system is continuing to address the needs that justified its introduction.

13.7 Access to CCTV images

PS22 The release of recorded footage or access shall be allowed to law enforcement in order to aid an investigation on the approval of the Security Manager. Any such request must be valid and lawful.

PS23 Images from CCTV cameras shall not be routinely disclosed to other third parties, without express permission being given by the Data Protection Officer who shall ensure that the disclosure observes the Data Protection Legislation.

PS24 The Security Manager will maintain a log of all disclosures of CCTV images.

PS25 No images from the CCTV system or recordings in any format shall be posted online or disclosed to the media.

13.8 Subject Access Requests

PS26 Data subjects may make a request for disclosure of their personal information and this may include CCTV images (data subject access request). A data subject access request is subject to the statutory conditions and should be made in writing and in accordance with UCL's data protection policy.

PS27 In order for UCL to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording; the location where the footage was captured; the precise location of the camera; and, if necessary, information identifying the individual, e.g. a description of clothing worn.

PS28 Images of third parties shall be obscured when disclosing CCTV data as part of a subject access request, or, where it is considered necessary to do so.

13.9 Complaints

PS29 Any questions about this policy or any concerns about UCL's use of CCTV should be raised with the Policy Contact [See Section 2] listed in the first instance. If the issue cannot be resolved, the complaint can be escalated to the Data Protection Officer.

PS30 Where this is not appropriate or matters cannot be resolved informally, employees should use UCL's formal grievance procedure.

14 Sanctions

This policy does not form part of a formal contract of employment with UCL, but it is a condition of employment that employees will abide by the regulations and policies made by UCL.

15 Approvals

Endorsed by the Security Working Group	**21 May 2018**
Endorsed by the Information Risk Management Group	**18 September 2018**
Approved by the Chair of the Information Risk Governance Group)	**11 December 2018**