CCTV PROCEDURES

To support Information Security Policy Framework

PROCEDURES

HERIOT-WATT UNIVERSITY
PROCEDURES FOR OPERATION OF CCTV ON UNIVERSITY PREMISES TO SUPPORT INFORMATION SECURITY POLICY FRAMEWORK

CONTENTS

PROCEDURES

1. INTRODUCTION

These procedures are applicable to all University staff. Their purpose is to ensure that the University Closed Circuit Television (CCTV) system is used to create a safer environment for staff, students and visitors to the University and to ensure that its operation is consistent with the obligations on the University imposed by the Data Protection Act 1998. For the purposes of the Data Protection Act 1998, the Data Controller is Heriot-Watt University.

The University has installed a comprehensive CCTV surveillance system across the Edinburgh campus for the principal purposes of preventing and detecting crime and promoting public safety.

The images from the CCTV system are monitored in the Security Control Room which is staffed by the University's Security Section. It is recognised that ancillary benefits of operating CCTV for this purpose may include reduction of the fear of crime generally and the provision of a safer public environment for the benefit of those who live or work within and visit the University.

CCTV Cameras which are located within individual academic buildings are the responsibility of the relevant Head of School or Institute, who is accountable for compliance with these procedures. Following the introduction of these procedures a programme will be agreed to manage the migration of all University CCTV cameras onto a common platform which will allow all recordings to be monitored from the Security Control Room.

Due to public concern surrounding a surveillance society, the use of CCTV surveillance must be consistent with respect for individuals' privacy. Other methods of achieving the objectives of a CCTV surveillance system will therefore be considered before installation of any CCTV camera on the University campus.

2. SCOPE

These procedures apply to all University CCTV cameras and equipment on the University's Edinburgh campus including systems managed by Professional Services, Schools and Institutes. Together, these comprise the University CCTV System. The University is the Data Controller for this system, determines the purpose of recording and is legally responsible and accountable for its use.

These procedures will be adapted to apply to all systems for which the University is the Data Controller on all campuses.

These procedures do not apply to audio-visual recordings made by members of the University community or visitors for their own private use on their own personally owned equipment. The University is not the Data Controller for such recordings. However, personal use of audio-visual recordings to harass or cause distress to others may be subject to disciplinary sanctions in accordance with other University regulations and policies governing the conduct of students, colleagues and other users and may also be in breach of criminal law.

3. OBJECTIVES

The University's CCTV surveillance system has been installed and is monitored for the following purposes:

- To assist in the prevention of crime and to aid public safety;

PROCEDURES

- To facilitate the detection of crime, identification, apprehension and prosecution of offenders in relation to crime and public order and for use in disciplinary investigations arising from alleged criminal activity or equivalent malpractice.

4 OPERATION OF THE UNIVERSITY'S CCTV SURVEILLANCE SYSTEM

4.1. The System

4.1.1. The system is operational and images are capable of being monitored twenty-four hours a day throughout the year. All CCTV cameras are configured to record images only: any sound recording facilities will be switched off or disabled.

4.1.2. The public and University community will be made aware of the presence of the system by appropriate signage which sets out the purposes for processing the CCTV images and identifies the University as the Data Controller responsible for processing those images.

4.1.3. The University is committed to fair, lawful, open and accountable use of CCTV. The University will not use CCTV for covert monitoring except in exceptional circumstances in which all of the following conditions are met:

- that there are grounds for suspecting criminal activity or equivalent malpractice such as behaviour which puts others at risk;
- that covert monitoring is the only practical way of obtaining evidence of this malpractice;
- that informing people about the monitoring would make it difficult to prevent or detect such wrongdoing;
- that the camera would be used only for a specific investigation, for a specified and limited time and be removed when the investigation has been completed.

Each such use of CCTV must be authorised in advance by the Secretary of the University and recorded in the central log of CCTV use by the Security and Operations Manager.

4.1.4. To ensure privacy, wherever practicable, the CCTV cameras are prevented from focusing directly or dwelling on domestic or residential accommodation. CCTV cameras located in or facing student accommodation will be trained on the exterior entrances and communal areas such as corridors and common rooms. Where it is not practicable to prevent the cameras from capturing images of such areas appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas.

4.1.5. The CCTV equipment and location of each camera will be chosen to meet the quality and image capture standards necessary to achieve the University's purposes for processing the images. The location and technical specification will take account of the field of vision of the camera, light levels and other environmental conditions and minimise the capture of images that are not relevant to the University's purposes. In procuring and deploying CCTV equipment, the University will take account of the technical standards set out by the Home Office Scientific Development Branch so that images are of sufficient quality for the University's purposes. The Home Office and the Information Commissioner's Office recommend that CCTV image quality must be fit for one or more of the following purposes: .

PROCEDURES

a) *Monitoring: to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.*
b) *Detecting: to detect the presence of a person in the image, without needing to see their face.*
c) *Recognising: to recognise somebody you know, or determine that somebody is not known to you.*
d) *Identifying: to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.*

Therefore, all University CCTV images processed for the identification, apprehension and prosecution of offenders in relation to crime and public order and for use in disciplinary investigations arising from alleged criminal activity or equivalent malpractice need to meet the quality and technical standards required for category d: identification.

CCTV equipment will be maintained and tested in accordance with a regular schedule. The Security and Operations Manager or his nominee will be responsible for testing the quality of images to ensure that recorded images and prints as well as live images are clear and fit for purpose, taking account of seasonal variations, such as the growth of spring and summer foliage or other factors that may obscure images, and to check that date and time stamps are correct.

4.1.6. Images captured by cameras will be recorded on equipment located securely within University buildings. The Security Control Room has monitoring equipment which allows Security officers to monitor live images from the cameras, and any transfer of images onto other media will only take place from within the Security Control Room in line with these procedures.

Although every reasonable effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the areas of coverage.

4.2. Security Control Room

4 2.1. Images captured by the system will be monitored in the self-contained and secure Security Control Room.

Access to the Security Control Room is strictly limited to the Duty Supervisors and other staff members authorised by the Security and Operations Manager. Police Officers may enter with the explicit consent of the Security and Operations Manager or the Duty Supervisor. Other persons may be authorised to enter the Security Control Room on a case-by-case basis with the explicit consent of the Security and Operations Manager with each visit being supervised at all times.

4.2.2. In the event of a major incident on campus, the Security and Operations Manager or Duty Security Supervisor will initially manage the incident from the Security Control Room until the Major Incident Management Team are advised and/or arrive on campus. On arrival, the management team will set up the Major Incident Control Room in the Heriot Room of the George Heriot Wing or Committee Room 1, Estate Services, as specified in the University Major Incident Plan. The Security Control Room will not be used by the management group for the purposes of managing the incident.

4.2.3. In an emergency, and where it is not reasonably practicable to secure prior

PROCEDURES

authorisation, the duty Security Supervisor may grant access to persons with a legitimate reason to enter the Security Control Room. Before access is granted to any person, the Security Supervisor must be satisfied with the identity of any visitor and the need for access.

4.2.4 Details of all visitors will be recorded in the Occurrence Log which is kept in the Security Control Room.

4.2.5. The Safeguard incident management system is used to record a log for each security incident including those captured on CCTV which are transferred to another medium, together with any consequential action taken.

4.2.6. Handling of images and information within the Security Control Room will be carried out in accordance with these procedures and the Data Protection Act 1998. The Security and Operations Manager will be responsible for compliance with section 4.2.5 above and for the development of working procedures within the Control Room to ensure such compliance.

5. MONITORING OF CCTV IMAGES

5.1. The Security and Operations Manager and where appropriate, the relevant Head of School, will ensure that all staff (including relief/temporary staff) are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance, including training in the data security requirements of these procedures and the Data Protection Act 1998, with input from the Head of Heritage and Information Governance.

5.2. The control of the CCTV Surveillance System will always remain with the University. However, at the discretion of the Secretary of the University or her nominee, the University may act on advice from the police in order to operate cameras during an incident to monitor potential public disorder, assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order. On each occasion the Police are assisted with their operations, a report setting out the time, date and detail of the incident will be submitted to the Security and Operations Manager and the original incident will be updated within the Safeguard system.

6. RECORDING OF IMAGES AND RESPONDING TO ACCESS REQUESTS

6.1. Control and Management of Recordings

6.1.1. All recording media used for the monitoring and capture of images on the University's CCTV system belong to and remain the property of the University.

6.1.2. The Security Control Room is supported by a digital recording system which stores images on appropriate media for fifteen days or until capacity is reached, whichever is the shorter period, and the images are then automatically erased.

6.1.3. Should it be necessary for images to be retained for release to a third party (including the Police) under the exemptions contained within sections 28(1), 29(1)(a) and (b) and/or 35(2)(a) of the Data Protection Act 1998, or retained for any other purpose in accordance with these procedures, for which the University's use of the system is registered with the Information Commissioner's Office, copies of those images will be transferred to a secure encrypted computer file.

PROCEDURES

6.1.4. Any file stored in line with 6.1.3 above shall be given a unique reference number by the person creating the file and a record made in an image tracking register contained within the Security Control Room.

6.1.5. Unless required for any of the reasons contained within Section 29(3) of the Data Protection Act 1968, recorded images will be retained in the Control Room for fifteen days, after that time the images are automatically overwritten by the recording equipment.

6.1.7. Where applicable, any recording medium will be cleaned before re-use to ensure that images are not recorded on top of images previously recorded.

6.1.8. All media containing recordings will be securely destroyed at the end of their lifespans.

6.2. Access to Recordings by Staff or Third Parties

6.2.1 It is important that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. These aspects of these procedures reflect the second and seventh Data Protection Principles of the Data Protection Act 1998.

6.2.2. Access to recorded images will be restricted to security staff and those who require access (for instance Health & Safety Services during accident investigations or Investigating Managers in situations where serious allegations about conduct or behaviour have been made), following the consent of the Security and Operations Manager, in order to achieve the purposes of using the equipment.

6.2.3. All requests by persons or organisations outside the University (including any bodies that may claim a statutory or legal right of access) for viewing or obtaining recordings must be assessed on a case by case basis by the Security and Operations Manager and the Data Protection Officer and the other relevant officers responsible for authorising the disclosure of student or staff personal data. Access will not be granted unless the responsible officers are satisfied that this is consistent with the obligations placed on the University by the Data Protection Act 1998.

6.2.4. All requests for access will be recorded using the University Disclosure Decision form [Appendix B] detailing:

- the date, time and purpose of the request,
- the decision to release or withhold the images and the reasons for the decision in each case,
- the date and time at which access was allowed/or disclosure made;
- the extent of the information accessed/disclosed;
- the name and role of the University officer making the decision to allow or withhold access,
- the name of the security staff member providing access.

6.2.5. The Security and Operations Manager is responsible for documenting each request in line with section 6.2.4 above on the Safeguard incident management system. Information will be logged at the Security Control Room. In all cases a copy of the record must be lodged with the responsible officers, listed in section 6.3.5 below, who maintain a complete, confidential record of all such cases on behalf of the Secretary of the University.

PROCEDURES

6.2.6. If the Security and Operations Manager considers that the assistance of a member of University staff is needed to identify a victim, witness or perpetrator in relation to a criminal incident, wherever practicable, the member of staff should be invited to view the images in the Security Control Room. If this is not possible, the Security and Operations Manager will copy the relevant images from the system onto a secure, encrypted file format and communicate this via the University's email system to selected staff on a targeted, need to know basis, or make the images accessible to appropriate staff via a secure Virtual Private network (VPN). The Security and Operations Manager will contact the recipient by telephone to communicate the password the encrypted file. As part of that decision, the wishes of the victim of an incident will, where possible, be taken into account.

6.3. Access by the Police

6.3.1. A police officer may request access to CCTV images held by the University either by viewing such data within the Security Control Room behind the main University reception or requesting a copy of the data. In most cases the police will request such access in response to a request by the University to investigate an alleged offence.

In cases where the police request University CCTV footage to investigate an alleged offence that the University has not reported, such requests for access to images are subject to the approval process set out in the Procedures for Liaison with Police on the Edinburgh Campus.

6.3.2 During working hours, requests for CCTV footage should be referred to the following officers:

Cases involving students:
Kathy Patterson, Academic Registrar & Deputy Secretary (ARDS),

Cases involving members of staff:
Ann Marie Dalton, Secretary of the University.

6.3.3 Outside of working hours requests for access to images should wherever possible be deferred until they can be considered by the appropriate University officer during working hours. In an emergency, if a request is straightforward and justifiable, for instance, a request for images of one incident involving criminal activity such as theft of a vehicle or equipment, the Security and Operations Manager or the Duty Security Supervisor may authorise disclosure to the police provided that:

- the request is in writing using the appropriate form md4 (04/11) (see Appendix A) signed by a Senior Police Officer, who must cite the relevant exemption/s to the non-disclosure provisions of the Data Protection Act; and

- the police demonstrate that the request is proportionate and necessary for the purposes of a specific crime enquiry.

In all other cases the Security and Operations Manager or deputy will report the request to the Secretary of the University or the Academic Registrar & Deputy Secretary or whichever senior officer is delegated to deputise for the Secretary of the University in her absence and seek authorisation to take appropriate action. These procedures will be supported by underpinning guidance which will set out

PROCEDURES

examples of straightforward and justifiable requests and those requiring escalation.

6.3.4. The Security Supervisor will complete form(s) ta/36 (03/06) and ta37 (06/11) (see Appendix D) to confirm the authenticity of the recordings and arrange for all data on recordings required for disclosure to be copied onto secure encrypted media.

6.3.5. The Security Supervisor must complete details of the request and any disclosure made in the Incident Report in the University's Safeguard electronic recording system.

For each disclosure request, a copy of the completed police request form, including the reasons given for the request, together with a University Disclosure Decision form [Appendix B] recording the decision to withhold or release the information, an encrypted copy of the recording disclosed, where applicable, and reasons for the decision must be lodged with the following responsible officers who maintain a complete confidential record of all such cases on behalf of the Secretary of the University.

Students:
Kathy Patterson, Academic Registrar & Deputy Secretary (ARDS),

Members of Staff:
Ann Marie Dalton, Secretary of the University.

6.3.6. Images and recordings requested for police investigations must be supplied directly to the police, not to any third party. Requests by individuals for their own images captured on CCTV will be dealt with in accordance with the section 6.4, below.

6.3.7 The Security and Operations Manager will liaise with the police to ensure that the University is informed of the outcome of the police investigation and authorise the police to destroy any University CCTV images and recordings when they are no longer required.

6.4. Access by Data Subjects

6.4.1. The University must comply with section 7 of the Data Protection Act, 1998, in informing individuals whether or not images and other information relating to them have been processed by the CCTV Surveillance System.

Individuals whose images are recorded have a right to make a request to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images.

In order to comply with a request the University needs to satisfy itself as to the identity of the person making the request for their own personal data. The person making the request also needs to provide enough information to enable University staff to locate their images.

Therefore Data Subjects wishing to make a subject access request (request for data about themselves) for CCTV images / recordings / information must apply in writing to the Data Protection Officer at the address given at the end of this Procedure.

In the request, the requestor must provide the following information:

PROCEDURES

6.4.1.1. Dates and times of the incident or their visit to the University with details of the location on the Edinburgh campus;

6.4.1.2. Two photographs – one full face and one side view;

6.4.1.3. Proof of identity (e.g. driving licence/passport containing a photograph);

6.4.1.4. Cheque or cash in the sum of £10.00;

6.4.1.5. Whether they require copies or view of the images in question.

6.4.2. A written decision will be sent to the data subject within five working days of receipt of the request. If access is agreed, such access will be provided within forty days of receipt of the request or, if later, on the date when the University receives confirmation of identification from the data subject.

6.4.3. In responding to a subject access request, University staff will use redaction tools to obscure images of other individuals in cases where releasing the unredacted images would involve an unfair intrusion into the privacy of the third parties concerned. Where the University is unable to comply with a subject access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

7. COMPLAINTS/BREACHES

7.1. Breaches of these procedures, whether by security staff, or other staff monitoring the system, or who have access to the monitored images, or who access images without authority to do so, will constitute Gross Misconduct and will result in disciplinary action being taken, which may lead to dismissal under the University's Disciplinary Code, Policy and procedures.

7.2. It is also recognised that other members of the University or third parties may have concerns or complaints in respect to the operation of the CCTV Surveillance System. Any concerns or complaints should, in the first instance, be addressed to the Security and Operations Manager who will follow the University Complaints Policy.

7.3. Concerns or queries relating to any aspect of compliance with the Data Protection Act, 1998, should be directed to the Data Protection Officer, who is the Head of Heritage and Information Governance.

8. RESPONSIBLE OFFICER

The Security and Operations Manager is responsible for the implementation of these procedures, in consultation with the Data Protection Officer.

9. MONITORING AND REVIEW

The Security and Operations Manager and the Data Protection Officer will monitor compliance with these procedures and the operational effectiveness of the University CCTV systems, reporting to the Information Governance and Security Group. These officers will initiate reviews of the procedure outwith the annual review cycle where necessary in the light of developments in the current legislation

PROCEDURES

which underpins the procedures.

The University Information Governance and Security Group will review these procedures annually. The review will consider the effectiveness of the procedures, and will take account of the views of stakeholders and relevant developments relating to the Data Protection Act, the statutory CCTV Code of Practice and other relevant legislation. Following review, these procedures will be revised and updated as appropriate.

10. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

These procedures should be read in conjunction with the following University Policies, Guidance and procedures:

Information Security Policy Framework
http://www.hw.ac.uk/documents/information-security-policy-framework.pdf

Data Protection Policy and Guidance
http://www.hw.ac.uk/about/policies/data-protection.htm

Procedures for Police Liaison at the Edinburgh Campus
http://www.hw.ac.uk/documents/police-liaison-procedures-edinburgh.pdf

Fair Processing Notice explaining the University's use of student data.
http://www.hw.ac.uk/registry/resources/studentpersonaldatastatement.pdf

Complaints Policy
http://www1.hw.ac.uk/registry/resources/complaint-policy.pdf

These procedures have been developed to comply with the Data Protection Act, 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents

and the **Information Commissioner's Office CCTV Code of Practice, 2008**
http://www.ico.org.uk/upload/documents/cctv_code_of_practice_html/index.html

Home Office Scientific Development Branch
CCTV Operational Requirements Manual (v0.4 55/06),
http://scienceandresearch.homeoffice.gov.uk/hosdb

11. FURTHER HELP AND ADVICE

For more information and advice about these procedures contact

Security and Operations Manager:
William J Taylor
Security and Operations Manager
Estates Services
Campus Services
Heriot-Watt University
Edinburgh EH14 4AS
Telephone: +44 (0)131 451 3404
Email: w.j.taylor@hw.ac.uk

PROCEDURES

Data Protection Officer:
Ann Jones
Head of Heritage and Information Governance
Governance and Legal Services
Heriot-Watt University
Edinburgh EH14 4AS
Telephone: +44 (0)131 451 3219
Email: foi@hw.ac.uk.

12. DEFINITIONS

CCTV	means Closed Circuit Television.
Control Room(s)	means the room(s) manned by security staff which contain the security, fire and CCTV systems.
Data Controller	means the organisation which decides the purposes for which and the manner in which any personal data are to be processed
Data Protection Officer	means the member of staff with oversight of organisational and technical measures and controls to comply with the Data Protection Act 1998.
Data Subjects	means an individual who is a subject of personal data.
HWU and **the University**	both mean Heriot-Watt University
Personal Data	means data which relates to a living person who can be identified from those data or other information that that the Data Controller holds or is likely to receive
Security and Operations Manager	shall mean, for the purposes of this Code, the member of staff with specific responsibility for management and control of the University's CCTV systems or his/her nominee.
System	means the University's CCTV Surveillance System including CCTV cameras.

13. PROCEDURES VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V. 5.5	01.07.2014	Secretary's Board in consultation with Information Governance and Security Group and CJNCC	Minor amendments and clarification of procedures in sections 4.2.2, 6.2.3 and 6.3.3 at the recommendation of the Secretary's Board on 01/07/2014

PROCEDURES

APPENDIX A

POLICE SCOTLAND

REQUEST FOR DISCLOSURE OF PERSONAL DATA

Under Sections 29 of the Data Protection Act, 1998

This form should be used when it is necessary to request personal data from another company / organisation.

The first box should be completed with the details of the organisation holding the data. The second and third boxes should detail the data required and the reason for the request. The form should be sent/given to the organisation and a copy retained by the officer/section making the request. Please note: the form can only be emailed if the rules for 'restricted' handling are followed i.e. the recipient's email address must be on the 'pnn', 'gsi', 'gsx' or 'nhs.net' network.

Organisation / Company: _____ Contact Name: _____

Address: _____

Telephone: _____

I am making enquiries on behalf of the Police Service of Scotland which are concerned with:

* (a) the prevention or detection of crime
* (b) the apprehension or prosecution of offenders
* (c) in order to protect the vital interests of the data subject or another person, in a case where-
  - (i) consent cannot be given by or on behalf of the data subject, or
  - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject.

Name: _____ Date of Birth: _____

Address: _____

_____

Nature of Enquiry: _____

_____

_____

Reason that the information is necessary:

_____

_____

_____

_____

I certify that the data is required for the reason(s) stated above. I understand that if any information on this form is omitted or wrong I may be committing an offence under Section 55 of the Data Protection Act, 1998.

Name and _____ Rank: _____

Signed: _____ Date: _____

Countersigned by Supervisor –

Name and _____ Rank: _____

Signed: _____ Date: _____

md4 *(04/11)*

PROCEDURES

APPENDIX B

Personal Data Disclosure Request: Decision Form

- Data Protection Act 1998 (DPA)

To be completed by the University officer responsible for the decision to release or withhold the personal data requested

1. Attach a copy of the applicant's disclosure request form, confirming that the form has been fully completed with the following information

Name, rank, signature and contact details of applicant, date of request	
Name, rank signature of supervisor authorising request, with date of authorisation	
Details of the individual/s (data subject/s) who is/are the subject of the personal data request	
Details of personal data requested	
DPA disclosure provisions cited by applicant	
Reason for request	

2. Decision:

Disclose	Withhold	Seek consent of data subject

3. Details of Decision

Reason for decision	
Personal Data Disclosed if applicable	
Method of disclosure	

4. Officer responsible for authorising disclosure/refusal of request

Name:		Signature:	
Role		Date	

PROCEDURES

5. Legal Authority under the Data Protection Act 1998 to disclose the personal data without consent

S 29 Crime and taxation: Personal data processed for any of the following purposes— .	
(1) (a) the prevention or detection of crime, .	
(1) (b) the apprehension or prosecution of offenders, or .	
(1) (c) the assessment or collection of any tax or duty or of any imposition of a similar nature	
Schedule 2 Conditions: (processing of any personal data)	
(2) The processing is necessary—. (a) for the performance of a contract to which the data subject is a party, or. (b) for the taking of steps at the request of the data subject with a view to entering into a contract.	
(3) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.	
(4) The processing is necessary in order to protect the vital interests of the data subject.	
(5) The processing is necessary—. (a) for the administration of justice, (aa) for the exercise of any functions of either House of Parliament,]. (b) for the exercise of any functions conferred on any person by or under any enactment, (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or. (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.	
(6) (1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.	
Schedule 3 Conditions: (processing of sensitive personal data)	
(1) The data subject has given his explicit consent to the processing of the personal data.	
2(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.	
(3) The processing is necessary	
a)in order to protect the vital interests of the data subject or another person, in a case where— (i) consent cannot be given by or on behalf of the data subject, or (ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or	
b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.	

APPENDIX C

POLICE SCOTLAND

POLICE SERVICE OF SCOTLAND

CERTIFICATE IN TERMS OF SECTION 283 of the CRIMINAL PROCEDURE (SCOTLAND) ACT 1995

I _____

Insert full name and designation

being a person responsible for the operation of a video surveillance system and a person who may sign a certificate under Section 283 of the Criminal Procedure (Scotland) Act 1995.

HEREBY CERTIFY:

(i) That the camera(s) is / are located at:

_____

Insert details of the location of the camera(s) (address) which are responsible for producing the video image.

(ii) That the nature and extent of my responsibility for the system is:

_____

Insert details of the nature and extent of the signatory's responsibility for the video surveillance system.

(iii) That the visual images recorded on the video tape(s) / computer recording medium / computer hard drive:

_____

Insert details of how the video tape(s) are identified, e.g. reference number(s).

are images recorded by the system of events which occurred at:

_____

Insert details of the place where the video images occurred.

on _____ at _____

Insert date on which the video images occurred — *Insert time at which the video images occurred*

Signed: _____ Date: _____

NOTE TO ACCUSED

If a notice is not served by you under Section 283(2) of the said Act not more than 7 days after the date of services of this certificate, the evidence contained in this certificate shall be sufficient evidence of the facts contained in the certificate

ta36 *(03/06)*

[1]

CA/ /
CR/ /
Inc No.
TSU/FCU Ref:

POLICE SERVICE OF SCOTLAND

CERTIFICATE OF AUTHENTICATION

In terms of Section 279 of the Criminal Procedure (Scotland) Act 1995

certified copy of audio/video/digital media
by person in possession and control of original

I [2] _____

_____

being the person who was on (or in between)[3] _____

in possession and control of the original of the copy audio/video/digital media, on which this certificate is attached hereby certify that it is a true copy of the original, which is in my possession and control.

[4] List and describe audio/video/digital media

Description of Original

Description of Copy

Signed: _____ **Date:** _____

1 Insert any known reference number
2 Insert name, address and, where appropriate, title of office held, or other designation
3 Insert date when there was possession and control of audio/video/digital media or, where appropriate, specify relevant period
4 Include in the descriptions any reference that is appended to the audio/video/digital media which reliance is being placed and record the locus where the audio/video/digital media was removed

ta37 *(06/11)*