CCTV Policy

1. Introduction

1.1 The University believes that CCTV is a powerful tool to assist with efforts to enhance community safety, and that the operation of CCTV should be controlled to avoid the potential of misuse. The Information Commissioner's CCTV Code of Practice provides a framework for the operation of CCTV. The University supports this Code of Practice, which is applied in the context of Teesside University through this CCTV Policy & Procedure.

1.2 Any reference in this document to 'CCTV System', 'CCTV' or 'System' applies equally to the core University CCTV System (which predominantly operates outside University buildings) and to the supplementary CCTV system (of cameras within University buildings). The cameras constituting the core University CCTV System are actively monitored in the University's CCTV control room, whereas recordings on the cameras constituting the supplementary University system are viewed by operators in the control room only as required by security concerns and/or reports of an incident.

1.3 No cameras, including webcams, may be installed or operated on University premises by University students, employees or agents for the purposes of security or safety other than cameras linked to the core University CCTV system or the supplementary University CCTV system.

2. Objectives

2.1 This Policy aims to ensure that CCTV on Teesside University's premises is operated **to enhance safety, and the sense of safety**; and thereby assists in encouraging use of University facilities, through the following subsidiary objectives:

(1) To assist in deterring crime

(2) To assist in detecting crime and to provide evidential material for court proceedings

(3) To assist in the overall management of buildings and land within the boundaries of the University

(4) To assist in monitoring, and planning for, emergency operations; and to assist the Police, Fire, Ambulance and Civil Emergency Services with the efficient deployment of their resources to deal with emergencies.

2.2 This Policy aims to ensure that CCTV is used transparently and proportionately to achieve the objectives identified in Section 2.1, in compliance with the law and the Information Commissioner's CCTV Code of Practice.

2.3 The reference in 2.1 (3) to "the overall management of buildings and land" incorporates such matters as monitoring of traffic flow, car-park capacity, defects in bollard operation, defects in lighting, and damage to buildings.

3. Core Obligations

3.1 The University will identify the locations of all cameras connected to the University's CCTV System and will monitor, and manage, images shown on these cameras in accordance with this Policy and the associated Procedure.

3.2 All staff and students of the University are subject to the CCTV Policy and are required to contribute, on request, to the application of this Policy.

3.3 Staff who have been designated as having responsibility for the management and the operation of the CCTV system are required to undertake their responsibilities strictly in accordance with this Policy, and the associated Procedure. Such staff are required to operate the CCTV system fairly, within the law, and only for the objectives identified in this Policy.

4. Guidance

4.1 This Policy is accompanied by a Procedure and a Manual which regulate the operation of CCTV.

4.2 Guidance on the application of this Policy and the associated Procedure is available from the Head of University Services or the Security Manager.

4.3 Further guidance on the practices and procedures necessary to comply with this Policy and Procedure is available from the Legal Services Division of the Academic Registry, and is accessible from the Legal Services intranet pages.

5. Responsibilities

5.1 Teesside University is the "data controller "of the system and the "owner" of the data generated by the system.

5.2 Overall responsibility for the implementation of the Policy has been delegated by the Vice-Chancellor to the University Secretary & Registrar. The University Secretary and Registrar has delegated initial responsibility for compliance matters to the Assistant Director (Legal Services), and day-to-day management of the data to the Security Manager (Campus Facilities).

5.3 Breach of this Policy and the associated Procedure may result in disciplinary action being taken in accordance with the University's Staff Disciplinary Policy and Procedure.

6. Human Rights

6.1 The University recognises that operation of the University CCTV system may be considered an infringement on privacy. The University acknowledges its obligations under the Human Rights Act 1998. The University also recognises its obligation to provide a safe environment for staff, students and visitors; and regards the use of CCTV within the University as a necessary, proportionate and suitable tool.

6.2 The CCTV system will only be used as a proportional response to identified problems and may only be used insofar as is necessary, in the interests of national security, public safety, the prevention and detection of crime or disorder, the protection of health, the protection of the rights and freedoms of others, the management of buildings and land, and assistance in the resolution of a factual disagreement which emerges during investigation of a grievance, complaint or disciplinary allegation.

6.3 The University CCTV system shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

7. Data Protection

7.1 The operation of the system has been registered with the Information Commissioner's Office in accordance with current Data Protection legislation

7.2 All personal data will be processed in accordance with the Principles of the Data Protection Act 1998 which include, but are not limited to:

i. All personal data will be processed fairly and lawfully (The definition of 'processing' covers 'obtaining')

ii. Personal data will only be processed for the purpose specified

iii. Personal data will be adequate, relevant and not excessive

iv. Personal data will be accurate and where necessary kept up to date

v. Personal data will be held no longer than necessary

vi. Individuals will be allowed access to information held about them and, where appropriate, will be permitted to correct or erase it

vii. Procedures will be implemented to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.

8. Release of Personal Data, Following a Personal Request for Information

8.1 Any request from an individual for the disclosure of personal data under the Data Protection Act, or for disclosure under the Freedom of Information Act, which he/she believes is recorded by virtue of the system, should be made, in the first instance, to the Legal Services Division of the Academic Registry.

8.2 Sections 7 and 8 of the Data Protection Act 1998 (rights of data subjects and others) shall be followed in respect of every request.

8.3 Any person making a request must be able to prove his/her identity and provide sufficient information to enable the data to be located.

8.4 The Assistant Director (Legal Services) and/or designated staff in the Legal Services Division are authorised to view CCTV images in order to process a Subject Access Request.

8.5 If a request can only be complied with by identifying another individual, or several individuals, arrangements must be made to safeguard the rights of that individual or individuals, such as obtaining permission from that individual or individuals or blocking of the image of that individual or individuals.

8.6 Where the Assistant Director (Legal Services), or designated staff in the Legal Services Division, authorises a viewing of a CCTV image by the individual whose personal data is recorded on the image, that individual may be accompanied during the viewing by a friend or by a representative from the individual's Trade Union.

8.7 Authorised viewings of personal data will normally take place in the Security Manager's Office.

9. Release of Personal Data as Required by Law

9.1 As required by law, the Security Manager may authorise Security Personnel to release personal data to members of the police service, or other agency having statutory authority to investigate and/or prosecute offenders.

9.2 Exemptions to the non-disclosure provision of information are provided in section 29 of the Data Protection Act, which allows that personal data processed for the purposes of

- The prevention or detection of crime
- The apprehension or prosecution of offenders

are exempt from the non-disclosure provisions in any particular case, "to the extent to which the application of those provisions would be likely to prejudice any of those purposes". Each and every application will be assessed on its own merits and 'blanket exemptions' will not be applied.

9.3 Members of the police service, or other agency having a statutory authority to investigate and/or prosecute offenders, may release to the media details recorded by the University, only in an effort to identify alleged offenders, or

potential witnesses, and only in accordance with their responsibilities as the new controller of the data.

10. Release of Personal Data to a Person who is not the Data Subject

10.1 A University Senior Manager* who is investigating a complaint, grievance, or disciplinary allegation, under a formal University process, must seek authorisation from the University Secretary and Registrar for release of the personal data contained in an image which has been obtained during surveillance of the campus, in accordance with the objectives stated in Section 2 of this Policy.

10.2 The University Secretary and Registrar may grant such authority, in writing, where he/she is satisfied, either:

a) that there is prima facie evidence of an allegation which exists independently of the image, and prior to the request for authorisation or

b) that the allegation relates to criminal activity or

c) that both parties have agreed that it would be beneficial for the University Senior Manager to view the image, or

d) that one (or more) party has already viewed the image (having submitted an application to view on the grounds of being recorded in the image).

10.3 In the absence of the University Secretary, the Vice-Chancellor may appoint another member of the Vice-Chancellor's Executive to act in place of the University Secretary and Registrar.

* *(For the purposes of these Regulations, a "University Senior Manager" is a School Manager, an Assistant Dean, an Assistant Director or a person of more senior status.)*

11. Complaints

11.1 Any student, member of staff or the general public wishing to register a complaint with regard to any aspect of the system may do so by contacting the Head of University Services in the first instance. Data Protection concerns may be referred to the Senior Administrator (Records Management).

11.2 Should the matter remain unresolved, a formal complaint may be submitted to the Director of Campus Facilities. The issue may be investigated under the Student Complaint Procedure, the Staff Grievance Procedure, or the special procedure for consideration of data protection matters, culminating in an appeal to the DPA/FOI Complaints Panel.

12. Copyright

The University retains ownership of copyright and of all material recorded by the system.

13. Relationship with Existing Policies, Standards and Legislation

This Policy and the CCTV Procedure take account of the University's Data Protection Policy, the Information Commissioner's CCTV Code of Practice, and the following legislation:

- Criminal Procedures and Investigations Act 1996
- Human Rights Act 1998
- Data Protection Act 1998
- Crime and Disorder Act 1998
- Equalities Act 2010

14. Definitions

In this Policy and Procedure, the phrases "disclosure of data", and "release of data" could incorporate a viewing of personal data and/or production of a copy of the personal data. The presumption under which this Policy and Procedure operates is that the viewing of data is sufficient for most circumstances. The release of a copy of personal data may only be authorised by the Assistant Director (Legal Services), the University Secretary and Registrar, or other nominee of the Vice-Chancellor.

CCTV Procedure

This Procedure accompanies the University's CCTV Policy which regulates the operation of Teesside University's CCTV system. The purpose of the CCTV Procedure is to support the objectives of the Policy by outlining how the University will implement the CCTV Policy.

Extract from Teesside University CCTV Policy

2. **Objectives**

2.1 This Policy aims to ensure that CCTV on Teesside University's premises is operated **to enhance safety, and the sense of safety**; and thereby assists in encouraging use of University facilities, through the following subsidiary objectives:

(1) To assist in deterring crime

(2) To assist in detecting crime and to provide evidential material for court proceedings

(3) To assist in the overall management of buildings and land within the boundaries of the University

(4) To assist in monitoring, and planning for, emergency operations; and to assist the Police, Fire, Ambulance and Civil Emergency Services with the efficient deployment of their resources to deal with emergencies.

CONTENTS

1. General Principles

1.1 Lawful – The system will be operated in accordance with the law, including, in particular, the Data Protection Act 1998 and the Human Rights Act 1998. The CCTV system may not be used where the privacy of individuals would clearly be violated, provided a criminal offence is not taking place.

1.2 Restricted Application – The system shall be operated fairly, within the law, and only for the purposes stated in the CCTV Policy. Any individual or authority/organisation utilising the CCTV system must comply fully with this Procedure and will be held accountable under the CCTV Policy and this Procedure.

1.3 Overt – The location of all cameras is stated in this document under Annex A and is available to the public. The Security Manager is required to ensure that Annex A and associated notices are kept up to date. The CCTV system will not be used for covert surveillance.

1.4 Balanced – The University will balance the public interest in achievement of the objectives of the CCTV system and the public interest in the operation of the CCTV system, including the security, transparency and integrity of all operational procedures in relation to CCTV. Consequently, a formal structure has been put in place, including a complaints procedure, by which it can be demonstrated that the CCTV system is accountable, and is also seen to be accountable.

2. Cameras and Coverage

2.1 The areas covered by the University's CCTV system, to which this Procedure refers, are public areas and areas within the responsibility and/or perimeter boundaries of Teesside University, including within University buildings.

2.2 The number and location of all of the cameras is detailed at Annex A.

2.3 Signs will be placed at the main entrance points to the University to indicate:

- The presence of CCTV
- The purpose of the CCTV system
- Ownership of the system
- Contact details

Signage will also be placed at entrances to the buildings where internal CCTV cameras are in operation.

2.4 Some cameras may be enclosed within all-weather domes for aesthetic or operational reasons, but the presence of cameras connected to the University's CCTV system will be identified by appropriate signs.

2.5 On occasions, transportable or mobile cameras connected to the University's CCTV system may be temporarily sited within the boundaries of the

University. The use of such cameras, and the data produced, will conform to the objectives of the University's CCTV system and will be governed by the University's CCTV Policy and Procedure.

3. Monitoring and Recording Facilities

3.1 The central security control room (referred to as "the control room"), staffed by CCTV operators, is located on the ground floor of the Library.

3.2 University CCTV operators are able to record images in real-time, replay images, and produce hard copies of recorded images, in accordance with this Policy and Procedure. This applies equally to images derived from the core system and from the supplementary system, but images from the supplementary system are not normally viewed in real time. Viewing and recording equipment may only be operated by trained and authorised operators.

3.3 The Security Manager may view all cameras from his Office, but cannot control the movement of cameras from this location.

3.4 In certain circumstances, University staff other than the CCTV operators may be granted viewing rights (live images only) for one or more cameras on the supplementary CCTV system. Applications for the right to view should be submitted in the first instance to the Security Manager using the form at Annex F. The right to view such a camera does not entail the right to control the camera, which remains solely with the CCTV operators in the control room.

3.5 In certain circumstances, in accordance with a Concordat and associated Protocols with Middlesbrough Council, images obtained on the core CCTV System may be viewed by CCTV operators in Middlesbrough Town Centre CCTV control room and by CCTV operators in Cleveland Police Headquarters. The Middlesbrough Town Centre CCTV control room may spot record an image in real time for the purposes of continuity of evidence.

4. Operation of the System

4.1 All persons operating CCTV cameras must act with the utmost probity at all times. Operators are required to sign a declaration of confidentiality (Annex B).

4.2 The Security Manager is required to provide all individuals operating the CCTV system with a copy of the CCTV Policy and Procedure. All relevant staff are required to sign to confirm that they fully understand their obligations as set out in the CCTV Policy and Procedure.

4.3 A Manual containing technical instructions on the use of the equipment will be housed in the control room.

4.4 The control room and monitoring system must be staffed, at all times, by at least one officer. Any unauthorised use or abandonment of the University

control room and its systems and equipment for any purpose whatsoever (apart from evacuation in an emergency) may amount to gross misconduct under the University's Staff Disciplinary Procedure. If the control room must be vacated in an emergency, for safety or security reasons, the Manual must be followed (Annex D).

4.5 Only members of staff authorised by the University to operate the CCTV system may have access to the operating controls (subject to 4.7 and 4.8 below). Those operators will have primacy of control at all times, including times where images are authorised to be viewed in the Town Centre CCTV control room.

4.6 When, in accordance with the Concordat and Protocols with Middlesbrough Council, permission has been granted by the primary control officer on duty at Teesside University for Middlesbrough CCTV control room to view a specific camera on the University's core system, this authorisation must be recorded on the daily occurrence log in the University control room.

4.7 The Police may make a request to assume partial direction of the system to which this Procedure applies. Only requests made on the written authority of a police officer, not below the rank of inspector, will be considered. Any such request will only be granted on the personal written authority of the Security Manager, subject to consultation and approval from the University Secretary and Registrar, or the Director of Campus Facilities. In the event of such a request being permitted, the monitoring room will continue to be staffed and the equipment operated by the Duty University CCTV controller. The controller will then operate the system under the direction of the police officer(s) designated in the written authority.

4.8 In very extreme circumstances, the Police may request control of the system in its entirety, including the staffing of the Control Room and the personal control of all associated equipment, to the exclusion of the system representatives. Any such request must be passed to the Security Manager, who will consult personally with the University Secretary and Registrar (or another Member of the Vice-Chancellor's Executive). A request for total exclusive control of the system must be made in writing by a police officer, not below the rank of Assistant Chief Constable, or person of equal standing.

5. Maintenance of the System

5.1 To ensure compliance with the Information Commissioner's Code of Practice, and to ensure that images recorded continue to be of appropriate evidential quality, the system shall be maintained in accordance with the requirements of the procedural manual under a maintenance agreement. User requirements can be maintained by a member of Security Personnel. Faults will need to be maintained by a CCTV Engineer.

5.2 The maintenance agreement will make provision for:

- regular service checks on the equipment, including cleaning of any all weather domes or housings, checks on the functioning of the equipment

and any minor adjustments that need to be made to the equipment to maintain picture quality.

- regular overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.
- "emergency" attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

5.3 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem, depending upon the severity of the event and the operational requirements of the system.

5.4 Appropriate records of faults must be maintained by the Security Manager in respect of the functioning of the cameras/system and the response of the maintenance organisation. (Annex C-1)

6. Access to, and Security of, Control Room and Associated Equipment

6.1 Only authorised operators who have been certified as appropriately instructed may operate any of the equipment located within the control room – subject to 4.7 and 4.8 above. A list of all authorised operators will be maintained in the control room by the Security Manager. An authorised operator must be present at all times when the equipment is in use.

6.2 The control room must be secured at all times. The entrance door to the control room must be fitted with a device to restrict entry from outside, and this must be used by authorised operators to maintain the security of the control room.

6.3 The following are authorised to visit the control room:

The Vice-Chancellor
The University Secretary and Registrar
The Assistant Director (Legal Services)
The Senior Administrator (Records Management)
The Director of Campus Facilities
The Assistant Directors of Campus Facilities
The Head of University Services
CCTV/Alarm engineers
University Library cleaning staff
Estates "on-call staff"
Police in the pursuance of their duties

The names of such visitors must be recorded, and visitors must be accompanied at all times by an authorised operator or the Security Manager.

6.4 Public access to the control room will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the Security Manager or the Head of University Services. Any such visits will be conducted and recorded in accordance with this Procedure.

6.5 Regardless of their status, all visitors to the control room will be required to read the declaration of confidentiality prior to signing the visitors book. (Annex C-2). Refused visitor details will also be recorded in the visitors book. Duty controllers must be satisfied that visitors can be accurately identified and that the purpose of their visit is valid.

7. Management of Recorded Material

7.1 For the purposes of this Procedure, "recorded material" means any material recorded by, or as a result of, the technical equipment which forms part of the system, but specifically includes images recorded digitally, or on video tape, or by way of video copying, inclusive of video prints. Every recording obtained using the system has the potential of containing material that may be admitted as evidence in a court of law at some point during its life span.

7.2 It is of the utmost importance that, irrespective of the format of the images obtained from the system, recorded material is treated strictly in accordance with this Procedure from initial recording to date of destruction. All movement and usage of material must be recorded (Annexes C-3, C-4, C-5, C-7).

7.3 Access to, and the use of, recorded material must be strictly in pursuance of the purposes defined in the University's CCTV Policy.

7.4 Recorded material may not be copied, sold or otherwise released or used for commercial purposes, personal use, or for the provision of entertainment.

7.5 All material recorded by the system will be retained for between 14 and 22 days (depending on the system) before being overwritten or erased. Recordings may only be retained beyond this period in the following circumstances:

- Where evidential material exists which is likely to be required by the Police. (This should be kept for duplication and subsequent production in court.)
- Where material is required following a Subject Access Request submitted within 14 days of the incident.
- Where material is required as part of a Freedom of Information Request
- Where the evidence is required under a court order.
- Where the Vice-Chancellor, the University Secretary, or the Assistant Director (Legal Services), informs the Security Manager that the maintenance of the material is in the interests of the University, and in accordance with the CCTV Policy.

In these circumstances, the material will be copied to a disc.

7.6 To ensure the quality of recorded material, only discs/tapes that have been specified for the sole use under Teesside University's CCTV system may be used. Each tape/disc will have its own unique identity number.

7.7 Each tape/disc will be magnetically erased/wiped –

- Before re-use

- Before destruction
- At the end of its life (12 months or earlier, if necessary)

7.8 The destruction of tapes /discs is to be recorded in the Data Destruction Register. (Annex C-6)

7.9 Images from every camera will be recorded continuously throughout a 24-hour period. Video tapes will be changed daily at 00.01hours. No tape, disc, print or still image may be retained beyond the 14/22 day period, other than in those special circumstances identified in 7.5 above.

7.10 All recorded images will be identified by camera number, date recorded and time group. Images may only be reviewed by University security officers, Security Manager, or by such other persons as are authorised by this Policy/Procedure. (Annex C-7)

7.11 Media prints will not be taken as a matter of routine. Justification must be provided for each print. Details of all media prints will be recorded (see Annex C-3)

7.12 In the event of any recorded material being required for evidential purposes, the procedures outlined in the procedure and manual must be strictly complied with.

8. Request for Information/Release of Data

8.1 Members of the University community and general public who believe their image has been captured by the system have the right to view relevant footage at a time convenient to themselves and to the University. To this end, an individual, and/or his/her legal representative, may request a viewing or a copy of the footage by writing to the University's Data Protection Co-ordinator. An administrative fee is payable for such viewing. (Annex E)

8.2 Requests for the release of personal data generated by this CCTV system should be directed to:

Data Protection Co-ordinator
Legal Services Division of Academic Registry
Teesside University
Middlesbrough
TS1 3BA

8.3 Principles 7 and 8 of the Data Protection Act 1998 (rights of data subjects and others) shall be followed in respect of every request.

8.4 Any person making a request must be able to prove his/her identity and provide sufficient information to enable the data to be located. To this end, the written request should be accompanied by name, address and proof of identify (photocopy of passport ID page, driving license, birth certificate or staff card).

8.5 On receipt of fee payment, the University will make every effort to reply to a request within 40 days. However, there may be some circumstances where the University requires further information, which will be requested within the 40 day period.

8.6 If the request can only be complied with by identifying another individual, permission from all parties must be sought first.

8.7 In complying with the national standard for the release of data to third parties, the University will, as far as is reasonably practicable, safeguard the individual's right to privacy, and will give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and should be used only for the purposes defined in this code
- Access to recorded material will only take place upon completion of a declaration of confidentiality.
- The release or disclosure of data for commercial or entertainment is specifically prohibited.

8.8 Members of the police service, or other agency having a statutory authority to investigate and/or prosecute offenders, may release to the media details recorded by the University only in an effort to identify alleged offenders or potential witnesses, and only in accordance with their responsibilities as the new controller of the data.

8.9 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must only be shown after prior approval for disclosure is granted by the Assistant Director (Legal Services) or person of equivalent status.

9. Responsibilities

9.1 Security Manager

The Security Manager will:

- Ensure that the Policy and Procedure are adhered to.
- Ensure that there is no breach of Security.
- Ensure that the functions of the CCTV system are implemented.
- Ensure that operators are supervised and developed.
- Ensure that the interests of the University are upheld in accordance with the terms of the Policy, Procedure and Code of Practice.
- Ensure that all faults relating to the system and any associated equipment forming part of the CCTV system are reported and adequately maintained and developed.
- Consider reports from the operators detailing the state of readiness of the equipment and the day-to-day and long-term operation of the system.

- In consultation with the operators and other relevant individuals, investigate and propose alterations, additions or amendments to the system.
- Liaise with relevant staff to ensure that CCTV Policy and Procedure remains compliant with legislation.
- Facilitate viewing requests, including making arrangements to copy footage for potential viewings, as requested by Legal Services.
- Ensure that operators and other relevant staff are regularly reminded about the contents of the Policy and Procedure, and any updates.
- Ensure destruction of images, in accordance with protocols.
- Monitor and supervise the daily procedural instructions, security of data and confidentiality.
- Ensure that at all times operators of the CCTV system carry out their duties in an efficient and responsible manner. This will include regular checks and audit trails to ensure that any documentation is relevant and up to date.

9.2 **Operators**

Operators are responsible for taking appropriate action to deal with incidents detected through use of the system, and for keeping records, as required by this Handbook.

Operators must:

- Carry out their duties in accordance with the Policy, the Procedure, and managerial instructions.
- Control and operate the cameras and equipment forming part of the system with proficiency.
- Ensure that information recorded by the system or operator (spot recording) is accurate, adequate, relevant and does not exceed that necessary to fulfil the purpose of the system.
- Justify decisions to view or record any particular individual, group of individuals or property, when requested by the supervisor or manager.
- Regularly refresh their knowledge of the contents of the CCTV Policy and Procedure, and manuals.

10. Discipline

10.1 Staff or students who impede implementation of the CCTV Policy may be subject to disciplinary proceedings.

10.2 Breach of the CCTV Policy, Procedure or any aspect of confidentiality by individuals with specific responsibilities under the terms of the CCTV Policy and Procedure may be subject to University's Staff Disciplinary Policy.

10.3 Any unauthorised use or abandonment of the control room, its systems and/or equipment, for any purpose whatsoever, (apart from evacuation in an emergency) may amount to gross misconduct under the University Staff Disciplinary Procedure.

11. Complaints

11.1 Any student, member of staff or the general public wishing to register a complaint with regard to any aspect of the system may do so by contacting the Head of University Services in the first instance. Data Protection concerns may be referred to the Senior Administrator (Records Management).

11.2 Should the matter remain unresolved, a formal complaint may be submitted to the Director of Campus Facilities. The issue may be investigated under the Student Complaint Procedure, the Staff Grievance Procedure, or the special procedure for consideration of data protection matters, culminating in an appeal to the DPA/FOI Complaints Panel.

12. Annexes

Annex A – Camera Locations
Annex B – Declaration of Confidentiality
Annex C – Relevant Documentation
Annex D –Control Room Evacuation Guidelines
Annex E – Personal Information Requests
Annex F - Remote Viewing Authorisation (Internal CCTV Only)

Annex A-1

Teesside University

External CCTV Camera Locations

Number	Camera Location	Type
01	Front corner house 20 King Edward square	PTZ
02	Rear corner house 12 King Edward Square	PTZ
03	Front right corner the Meteor Building	PTZ
04	Between house 5 and 6 King Edward Square	PTZ
05	South West Corner the Brittan Building	PTZ
06	West side Student Centre	PTZ
07	East side Student Centre	PTZ
08	Quadrangle car park	PTZ
09	Berkeley car park	PTZ
10	Rear doors Middlesbrough Tower	Static
11	Spare	Nil
12	East side Stephenson Building	Dome
13	East end the Harvard car park	Dome
14	The Princeton car park	Dome
15	Front South West corner the Athena building	Dome
16	The Cornell car park	Dome
17	North East corner the Columbia (OLTC) car park	PTZ
18	North East corner Student Union car park	PTZ
19	Underneath Student Union	Dome
20	North west corner Student Union	PTZ
21	South East corner Library	PTZ
22	North West corner Library	Dome
23	North side Sage car park	PTZ
24	Next to North East corner Centuria North Building	PTZ
25	South East corner Centuria North Building	Dome
26	Rear Victoria buildings South West corner	PTZ
27	Front of Victoria building North East corner	PTZ
28	South East corner Woodlands Hall Five	PTZ
29	East Side Mercuria building (Penn car park)	PTZ
30	South West corner Mercuria building (Penn car park)	PTZ
31	Middletown car park	Dome
32	Near to South West corner Olympia sports pitch on footpath	Dome
33	Rear gate Parkside West	PTZ
34	Gable end House eight Parkside West	PTZ
35	Corner House Sixteen Parkside West	PTZ
36	West end car park, Parkside East	PTZ
37	North West corner Parkside Halls	PTZ
38	North East corner house seventeen Parkside East	PTZ
39	North East corner Parkside Hall	PTZ
40	North East corner Parkside East	PTZ
41	South East corner Parkside Hall	PTZ
42	North East corner Centuria South	Dome
43	Main Entrance (South side) Centuria South	Dome
44	South West corner Centuria South	Dome
45	West side Centuria South	Dome
	External Cameras Clarendon car park	
01	North East pedestrian entrance	Static
02	Centre row (looking East)	Static
03	South row (looking East)	Static
04	North row (looking East)	Static
05	Centre row (looking West)	Static
06	South row (looking West)	Static
07	North row (looking West)	Static
08	North west, main car park entrance	Static
09	South east pedestrian entrance (Southfield lane)	Static

Annex A-2

Internal Camera Locations (All Static)

Athena

Athena 1 – 1	North Stairs		Athena 2 – 8	Room A2.06
Athena 1 – 2	GF >> S		Athena 2 – 9	Room A2.07
Athena 1 – 3	Room AG.06		Athena 2 – 10	Room A2.08
Athena 1 – 4	GF >> N		Athena 2 – 11	Room A2.09
Athena 1 – 5	South East Stairs		Athena 2 – 12	Landing 2nd Floor >> S
Athena 1 – 6	Reception Desk		Athena 2 - 13	Lifts 2nd Floor
Athena 1 – 7	North Entrance		Athena 2 - 14	Landing 2nd Floor >> N
Athena 1 – 8	Lifts/Foyer		Athena 3 - 1	Room A3.02
Athena 1 – 9	South Entrance Doors		Athena 3 – 2	Landing 3rd Floor >> N
Athena 1 - 10	South West Stairs		Athena 3 – 3	Lifts 3rd Floor
Athena 1 – 11	Bicycle Store		Athena 3 – 4	Landing 3rd Floor >> S
Athena 2 - 1	Corridor 1st Floor >> S		Athena 3 – 5	Room A3.10
Athena 2 – 2	Landing 1st Floor >> S		Athena 3 – 6	Room A3.09
Athena 2 – 3	Lifts 1st Floor		Athena 3 – 7	Room A3.08
Athena 2 – 4	Landing 1st Floor >> N		Athena 3 – 8	Room A3.07
Athena 2 – 5	Room A1.01		Athena 3 – 9	Room A3.06
Athena 2 – 6	Room A2.05		Athena 3 - 10	Corridor 3rd Floor >> S
Athena 2 - 7	Corridor 2nd Floor >> S			

Aurora House

Aurora 1	Store		Aurora 3	Reception Area
Aurora 2	Main Entrance/Lobby - Internal		Aurora 4	Main Entrance - External

Brittan

Mock Court - 4	Café/Brittan Entrance

Centuria North

Centuria N 1 - 1	Main Entrance		Centuria N 1 – 12	H1.41 North Corridor > W
Centuria N 1 – 2	Arena		Centuria N 1 – 13	H1.26 West Corridor > N
Centuria N 1 – 3	H0.44 North Corridor > E		Centuria N 1 – 14	H1.28 West Corridor > S
Centuria N 1 – 4	H0.46 North Corridor > W		Centuria N 1 – 15	H1.13 South Corridor > W
Centuria N 1 – 5	H0.28 West Corridor > N		Centuria N 1 - 16	H1.16 South Corridor > E
Centuria N 1 – 6	H0.32 West Corridor > S		Centuria N 2 - 1	Room H0.01
Centuria N 1 – 7	H0.16 South Corridor > W		Centuria N 2 – 2	Room H0.53
Centuria N 1 – 8	H0.16 South Corridor > E		Centuria N 2 – 3	Room H0.49
Centuria N 1 – 9	Stairs to 1st Floor		Centuria N 2 – 4	Room H0.46
Centuria N 1 – 10	PC Open Area		Centuria N 2 – 5	Room H0.43
Centuria N 1 - 11	H1.38 North Corridor > E		Centuria N 2 - 6	Room H0.38

Centuria South

Centuria S 1 - 2	HS 0.07 Recycling Store		Centuria S 2 - 1	1st Floor Lift Area
Centuria S 1 – 3	Ground Floor Dental Corridor		Centuria S 2 – 2	1st Floor Corridor >> West
Centuria S 1 – 4	South West Fire Exit		Centuria S 2 – 3	2nd Floor West Stairwell
Centuria S 1 – 5	Dental Reception		Centuria S 2 – 4	HS 2.12 Corridor >> West
Centuria S 1 – 6	Main Entrance		Centuria S 2 – 5	2nd Floor Corridor >> East
Centuria S 1 – 7	Ground Floor >> East		Centuria S 2 – 6	2nd Floor Stairs/Link Door
Centuria S 1 – 8	Ground Floor Lift Area		Centuria S 2 – 7	2nd Floor Lift Area
Centuria S 1 – 9	Ground Floor Link >> North		Centuria S 2 – 8	HS 2.20b Server Room
Centuria S 1 – 10	Plant Rooms Fire Exit		Centuria S 2 – 9	2nd Floor Corridor >> West
Centuria S 1 – 11	Forum Area Fire Exit		Centuria S 2 – 10	HS 3.12 Corridor >> West
Centuria S 1 – 12	East Fire Exit		Centuria S 2 – 11	3rd Floor Landing
Centuria S 1 – 13	1st Floor West Stairwell		Centuria S 2 – 12	3rd Floor Lift Area
Centuria S 1 – 14	1st Floor >> South		Centuria S 2 – 13	3rd Floor Corridor >> West
Centuria S 1 – 15	1st Floor >> East		Centuria S 2 – 14	3rd Floor West Stairwell
Centuria S 1 - 16	1st Floor Stairs/Link Doors			

Clarendon

Clarendon 1 - 1	Room CL1.08		Clarendon 2 – 4	Room CL1.92
Clarendon 1 – 2	Room CL2.52		Clarendon 2 – 5	CL1.06 Area
Clarendon 1 – 3	Room CL2.49		Clarendon 2 – 6	1st Floor Link (External)
Clarendon 1 – 4	Room CL2.18		Clarendon 2 – 7	SSSL Open Area
Clarendon 1 – 5	TBS Staff Door North		Clarendon 2 – 8	Room CL1.03
Clarendon 1 – 6	Link Stairs (Internal)		Clarendon 2 – 9	SSSL PC Area
Clarendon 1 – 7	Room CL2.57		Clarendon 2 – 10	NW Fire Stairs
Clarendon 1 – 8	CL2.05 Area		Clarendon 2 – 11	SE Fire Stairs
Clarendon 1 – 9	TBS Reception		Clarendon 2 – 12	SW Fire Stairs
Clarendon 1 – 10	TBS Open Area		Clarendon 2 – 13	SSSL Reception
Clarendon 1 – 11	Room CL2.19		Clarendon 2 – 14	GF Lobby Kiosk
Clarendon 1 – 12	CL2.58 Area		Clarendon 2 – 15	CL1.86 Area
Clarendon 1 – 13	Room CL2.58		Clarendon 2 – 16	Room CL2.07
Clarendon 1 – 14	Room CL1.87		Clarendon 3 - 1	Area CL2.09/2.06
Clarendon 1 – 15	Room CL1.90 (PC Lab)		Clarendon 3 – 2	Area CL2.12
Clarendon 1 – 16	TBS Staff Door South		Clarendon 3 – 3	Area CL2.61
Clarendon 2 - 1	Room CL1.86		Clarendon 3 – 4	Cameo Cafe
Clarendon 2 – 2	Room CL1.89A (Office)		Clarendon 3 – 5	Ground Floor Lobby
Clarendon 2 - 3	NE Fire Stairs		Clarendon 3 - 6	Bicycle Store

Constantine

ICT 1 – 11	C.L.T.		ICT 1 - 13	Room C G.17
ICT 1 – 1	AV Store CLT		ICT 2 – 12	Area CG.23
ICT 2 – 11	Area CG.11		ICT 1 – 12	Room C G.26
ICT 2 – 9	Area CG.14 > S		ICT 1 – 10	Room C 2.09
ICT 2 - 10	Area CG.14 > N		ICT 2 - 13	Area C2.10

Cook Building

Cook – 1	Workshop		Cook – 5	2nd Floor Landing
Cook – 2	Mill area door		Cook – 6	3rd Floor Landing
Cook – 3	Ground Floor Lobby		Cook - 7	4th Floor Landing
Cook - 4	1st Floor Landing			

Crime Scene House

CSH – 1	Briefing Room		CSH – 9	Dentist
CSH – 2	Kitchen		CSH – 10	Stairs
CSH – 3	Entrance		CSH – 11	Sam's Room
CSH – 4	Bathroom		CSH – 12	Shop
CSH – 5	Shower Room		CSH – 13	Bar
CSH – 6	Workshop		CSH – 14	Travel
CSH – 7	Solicitors		CSH – 15	Fire Room
CSH - 8	Nurse Bed		CSH – 16	Yard

Europa Building

Europa 1 – 1	West Doors CFE		Europa 2 - 8	CFE Room 2.31
Europa 1 – 2	Open Area CFE		Europa 2 – 9	CFE Room 2.31
Europa 1 – 3	East Stairs GF CFE		Europa 2 – 10	I.T. Corridor (0.02)
Europa 1 – 4	Lift area GF East CFE		Europa 2 – 11	I.T. Room 0.15
Europa 1 – 5	Room 1.36 CFE		Europa 2 – 12	I.T. Room 0.13
Europa 1 – 6	Room 1.34 CFE		Europa 2 – 13	I.T. Room 0.11
Europa 1 - 7	!st Floor Corridor >> West (1.40) CFE		Europa 2 – 14	I.T. Room 1.13
Europa 1 – 8	1st Floor Corridor >> East (1.39) CFE		Europa 2 - 15	I.T. Room 1.11
Europa 1 - 9	Room 1.33 CFE		Europa 2 - 16	I.T. Room 0.31 (CFE)
Europa 1 – 10	Room 1.31 CFE		Europa 3 - 1	Room IT 1.10
Europa 1 – 11	Stairs/Lift 1st Fl (1.38) CFE		Europa 3 – 2	Room IT 1.08
Europa 1 – 12	2nd Floor Stairs West CFE		Europa 3 – 3	OL Entrance
Europa 1 – 13	Room 2.43 CFE		Europa 3 – 4	OL Central Stairs
Europa 1 – 14	2nd Floor Corridor >East (2.46) CFE		Europa 3 – 5	Room OL-1
Europa 1 – 15	Room 2.42 CFE		Europa 3 – 6	Room OL-1
Europa 1 – 16	Room 2.40 CFE		Europa 3 – 7	Room OL-3
Europa 2 - 1	I.T. 1st Floor		Europa 3 – 8	Room OL-3

Europa 2 – 2	I.T. Ground Floor		Europa 3 – 9	Room OL-7
Europa 2 – 3	I.T. Stairs (1.01)		Europa 3 – 10	OL Fire Exit (NE)
Europa 2 – 4	CFE Room 2.39		Europa 3 – 11	Room OL-8
Europa 2 – 5	CFE Room 2.34		Europa 3 – 12	Room OL-8
Europa 2 – 6	CFE 2nd Fl Corridor >> West (2.45)		Europa 3 – 13	Room OL-9
Europa 2 - 7	CFE Stairs/Lift 2nd Floor		Europa 3 - 14	Room OL-9

Greig

Greig – 1	Entrance		Greig – 9	Room G0.46A
Greig – 2	Lobby		Greig – 10	South Exit (Disabled Ent)
Greig – 3	Oasis		Greig – 11	Room G1.07
Greig – 4	Room G0.57		Greig – 12	East Entrance Door (Columbia)
Greig – 5	Room G0.54		Greig – 13	Stores/Skip Area
Greig – 6	Room G0.31		Greig S - 1	Atrium
Greig – 7	NW Fire Exit Corridor		Greig S – 2	Server Room
Greig – 8	Disabled Access External		Greig S – 3	Server Entrance Corridor

Middlesbrough Tower

Mock Court – 3	Tower - Reception		ICT 3 – 11	M4.01/02 Entrance
ICT 1 – 14	Lift Lobby Area		ICT 3 – 13	Room M4.03
Mock Court - 1	Mock Court Room		ICT 3 – 6	Room M4.04
Mock Court – 2	South Entrance - Tower		ICT 3 – 9	Room M4.19
ICT 1 – 1	ICT Systems Entrance		ICT 3 – 2	Area M5.02 >S
ICT 1 – 3	Network Room		ICT 3 – 10	Room M5.04
ICT 1 – 4	Server Room		ICT 3 – 4	Room M5.05
ICT 1 – 5	South Stairs Tower		ICT 3 – 12	Lift Area 6th Floor
ICT 1 – 6	Front Stairs Tower		ICT 3 – 8	Area M6.09 >N
ICT 1 - 7	Room M1.31		ICT 3 – 1	6th Floor South Doors
ICT 2 – 5	Room M2.04		ICT 3 – 14	Room M7.04
ICT 2 – 6	Room M2.05		ICT 3 - 15	Room M7.04
ICT 1 – 15	2nd Floor Lobby (Estates area)		ICT 3 – 5	Area M7.04
ICT 1 - 16	2nd Floor Lift Area		ICT 3 – 7	Lift Area 7th Floor
ICT 2 – 2	Area M3.04		ICT 3 – 3	7th Floor South Stairs
ICT 2 – 7	Area M3.05		ICT 1 - 9	Room M10.13
ICT 2 – 4	Area M3.06		ICT 1 - 8	Room M10.14
ICT 2 – 1	Area M3.07		ICT 2 - 15	Lift Area 10th Floor
ICT 2 – 8	Area M3.09		ICT 2 - 14	South Stairs 10th Floor
ICT 2 – 3	Area M3.10			

Library

Library – 1	East Fire Exit (Double)		Library – 5	West Fire Exit (Single)
Library – 2	Ground Floor		Library – 6	Technicians Area
Library – 3	West Fire Exit (Double)		Library – 7	South Fire Exit
Library – 4	4th Floor		Library – 8	Counter area

Minerva

Minerva – 1	South Entrance		Minerva – 6	Room N 1.04
Minerva – 2	North Entrance		Minerva – 7	Room N 1.08
Minerva – 3	North Entrance		Minerva – 8	Room N 1.06
Minerva – 4	Room N 0.02		Minerva – 9	Room N 1.06
Minerva – 5	Room N 1.03			

Olympia

Olympia – 1	Lobby		Olympia – 8	Squash Court 1
Olympia – 2	GF Corridor (Squash Courts) > S		Olympia – 9	Squash Court 2
Olympia – 3	GF Corridor (Locker Area) > E		Olympia – 10	Balcony (Sports Hall)
Olympia – 4	Lounge		Olympia – 11	OLY2.01 (GPT 1)
Olympia – 5	1st Fl Corridor > W		Olympia – 12	OLY2.02 (GPT 2)
Olympia – 6	Data Analysis Lab (OLY 1.04)		Olympia – 13	Boulder Wall
Olympia – 7	Sports Pitch		Olympia – 14	Climbing Wall

Orion

Orion – 1	Lobby		Orion – 4	2nd Floor Corridor >>W
Orion – 2	GF Corridor >>W		Orion – 5	External Bin Store
Orion – 3	1st Floor Corridor >>W			

Parkside West

PSW – 1	Parkside Offices Lobby		PSW – 4	Server Room
PSW – 2	Server Room		PSW – 5	F/Exit Corridor
PSW – 3	Server Room			

Phoenix

Phoenix 1 – 1	North West Entrance		Phoenix 2 – 4	Room P2.08
Phoenix 1 – 2	Main Entrance		Phoenix 2 – 5	Room P2.09
Phoenix 1 – 3	Lift/North Doors Area		Phoenix 2 – 6	Room P2.10
Phoenix 1 – 4	Ground Floor Corridor >> East		Phoenix 2 – 7	Room P2.11
Phoenix 1 – 5	Room PG.13		Phoenix 2 – 8	Room P2.12
Phoenix 1 – 6	Ground Floor Corridor >> West		Phoenix 2 – 9	2nd Floor Corridor >> East
Phoenix 1 – 7	1st Floor Landing		Phoenix 2 – 10	2nd Floor Corridor >> West
Phoenix 1 – 8	1st Floor Landing/Lift Area		Phoenix 3 – 1	3rd Floor Landing
Phoenix 1 – 9	1st Floor Corridor >> East		Phoenix 3 – 2	3rd Floor Corridor >> East
Phoenix 1 – 10	Room P1.06		Phoenix 3 – 3	Room P3.06
Phoenix 1 – 11	Room P1.07		Phoenix 3 – 4	Room P3.07
Phoenix 1 – 12	Room P1.08		Phoenix 3 – 5	Room P3.08
Phoenix 1 – 13	Room P1.09		Phoenix 3 – 6	Room P3.09
Phoenix 1 – 14	Room P1.10		Phoenix 3 – 7	Room P3.10
Phoenix 1 – 15	1st Floor Corridor >> West		Phoenix 3 – 8	Room P3.11
Phoenix 2 – 1	2nd Floor Landing		Phoenix 3 – 9	Room P3.12
Phoenix 2 – 2	Room P2.06		Phoenix 3 – 10	3rd Floor Corridor >> West
Phoenix 2 – 3	Room P2.07			

Stephenson

Stephenson -1	Reception		Stephenson -7	Lecture Theatre (IC0.03)
Stephenson -2	Outer Lobby		Stephenson -8	IC 1.42
Stephenson -3	Ground Floor		Stephenson -9	MyPrint Machine (1st Floor)
Stephenson -4	Stairs (South)		Stephenson -10	IC 1.77
Stephenson -5	Lecture Theatre (IC0.03)		Stephenson -11	IC 1.60
Stephenson -6	Lecture Theatre (IC0.03)		Stephenson -12	North Fire Exit (Borough Road)

Students Union

Student Union – 1	North Entrance Door		Student Union – 8	Pool Tables/East Fire Exit
Student Union – 2	1st Floor Landing		Student Union – 9	Cash Point
Student Union – 3	Reception Desk		Student Union – 10	Hub
Student Union – 4	Shop Corridor		Student Union – 11	Terrace > West
Student Union – 5	Bar Ent/Area		Student Union – 12	Terrace > East
Student Union – 6	Games Machines		Student Union – 13	2nd Floor Landing
Student Union – 7	Bar Area			

Victoria

Victoria – 1	Reception		Victoria – 8	Room V0.02
Victoria – 2	Corridor GF Centre		Victoria – 9	Corridor GF East
Victoria – 3	Corridor GF East		Victoria – 10	Room V0.06
Victoria – 4	1st Floor West		Victoria – 11	Room V0.07
Victoria – 5	1st Floor East		Victoria – 14	F/Exit East (External)
Victoria – 6	Corridor GF West		Victoria – 15	F/Exit West (External
Victoria – 7	Room V0.01		Victoria – 16	Intercom

Waterhouse

Waterhouse – 1	Main Entrance		Waterhouse – 6	Room W1.09
Waterhouse – 2	Stairs W1.01		Waterhouse – 7	Room W0.04
Waterhouse – 3	W0.01 Corridor		Waterhouse – 8	Room W0.05
Waterhouse – 4	Fire Exit		Waterhouse – 9	Room W1.07
Waterhouse – 5	W0.09 Area		Waterhouse – 10	Room W2.02

Eastbourne Campus				
Eastbourne 1 - 1			Eastbourne 1– 9	
Eastbourne 1 – 2			Eastbourne 1 – 10	
Eastbourne 1 – 3			Eastbourne 1 – 11	
Eastbourne 1 – 4			Eastbourne 1 – 12	
Eastbourne 1 – 5			Eastbourne 1 – 13	
Eastbourne 1 – 6				
Eastbourne 1 – 7				
Eastbourne 1 – 8				

Saltersgill				
Saltersgill – 1			Saltersgill – 1	
Saltersgill – 1			Saltersgill – 1	

Annex B

Declaration of Confidentiality

Teesside University CCTV System

I, (……..……..…….... D.O.B ……...……..) am employed by (..... ……..……) in the capacity of ……. to perform the duty of CCTV Control Room Operator /Supervisor/Manager. I have received a copy of the Code of Practice and/or the CCTV Procedural Manual in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of that CCTV Code of Practice/Procedural Manual and understand that all duties which I undertake in connection with my employment must not contravene any part of the current code of practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the system or the content of the code of practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation any information which I may have acquired in the course of, or for the purposes of, my position within the CCTV control Room. I also understand this undertaking will apply for a period of one year after the cessation of my employment in connection with the CCTV control room.

In appending my signature to this declaration, I agree to abide by the Code of Practice/Procedure Manual at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or in the future.

Signed: .....

Print Name: .....

Witnessed: ..... Position: .....

Dated the ..... day of .....

Maintenance Log – External CCTV Cameras

Camera 1			
Camera Type		**Camera Location**	

Date of Fault	Description	Estates Ref	Date of Repair	Remarks

Control Room CCTV Equipment – General

Date of Fault	Description	Estates Ref	Date of Repair	Remarks

Maintenance Log – Control Room Recording Equipment

Equipment		**Function**	
Serial Number			
Date of Fault	**Description**	**Estates Ref**	**Date of Repair**

Maintenance Log – Internal Recording Equipment

Equipment		Function	
Serial Number		Cameras	
System Owner			

Date of Fault	Description	Date of Repair	Remarks

WARNING

RESTRICTED ACCESS AREA

Everyone, regardless of status, entering this area is required to complete an entry in the Visitors book.

Visitors are advised to note the following confidentiality clause and to understand that entry is conditional on acceptance of that clause.

CONFIDENTIALITY CLAUSE

'In being permitted entry to this area you acknowledge that you agree not to divulge any information obtained, overheard or overseen during your visit. An entry, accompanied by your signature in the Visitors book is your acceptance of these terms'

(Visitors Log Control Room)

Note: **In signing this visitors book all visitors to the University of Teesside CCTV Control Room acknowledge that personal details of those operating the system, is, and should remain confidential.**
You further agree not to divulge any information obtained, overheard or overseen during your visit.

Date	Name	Company/Dept	Signature	Time In	Time Out	Remarks

Serial No:

TEESSIDE UNIVERSITY SECURITY MEDIA PRINT REGISTER

Security Serial No		Date Produced	
Reason for Production			
Operator Name		Issued To	
Operator Signature		Signature	
Date		Date	

Security Serial No		Date Produced	
Reason for Production			
Operator Name		Issued To	
Operator Signature		Signature	
Date		Date	

Security Serial No		Date Produced	
Reason for Production			
Operator Name		Issued To	
Operator Signature		Signature	
Date		Date	

Security Serial No		Date Produced	
Reason for Production			
Operator Name		Issued To	
Operator Signature		Signature	
Date		Date	

Security Serial No		Date Produced	
Reason for Production			
Operator Name		Issued To	
Operator Signature		Signature	
Date		Date	

Note: Data Destruction Register is to be completed when printed media is returned to Security and no longer required for evidential purposes.

CCTV SPOT TAPE LOG

IMPORTANT. CHECK TAPE NUMBER CORRESPONDS

Tape Serial No:

VCR	SPOT

Part One

TAPE START				TAPE FINISH			
Tape S/N √	Erased √	Date & Time	Operator	Date & Time	Review √	Rewind √	Operator

Note 1: Part One (above) is used for recording spot tape usage. When the spot tape is Inserted/Removed from the system all relevant details should be entered in part one.

Note 2: Parts Two & Three overleaf are to be completed in respect of an incident requiring the tape to be used for evidential purposes. Part Four is to be completed when Spot & Copy Tapes are issued to Police.

Note 3: Data Destruction Register is to be completed when the spot tape reaches the end of its working life (12 months) and/or when a spot tape/copy tape (produced from the spot tape) is no longer required for evidential purposes and is to be destroyed.

Parts Two and Three are to be completed when a copy of an Incident is requested by the Police.

Part Two

INCIDENT DETAILS		
Report No/Log Entry Date & Time	Date & Time of Incident	Camera Number(s)

Brief Details	

Part Three

COPY TAPE PRODUCTION		Tape Serial No	
Date Produced:			
Produced By:			
Signature:			

Part Four is to be completed when tapes are issued to Police.

Part Four

Tapes Issued to Police					
Date:		S/O Name:		Signature:	
Spot Tape:					
Copy Tape:					
Issued To:					
Name		Signature		Date	

Additional Notes	

No tape is to leave the Control Room unless it is signed for.

DIGITAL CCTV EVIDENCE REGISTER

Sheet Ser No_____

MASTER	Serial No	
COPY	Serial No	

DVD PRODUCTION	
Date Produced	
Produced By	
Signature	

ISSUE DETAILS			
Issued By		Issued To	
Date		Date	
Signature		Signature	

Both Master & Working Copies to be Issued.

RECORDING DETAILS			
Recorder Location			
Camera No(s)		Date & Time of Incident	
Incident No/Reference			
Brief Details			

Notes:

- Data Destruction Register is to be completed when the DVD's are returned to Security and no longer required for evidential purposes.
- All DVDs that fail to record should be recorded in the Data Destruction Register and then destroyed
- **No DVD is to leave the Control room unless it is signed for.**

DATA DESTRUCTION REGISTER

DESTRUCTION NOTES

1. **DVD/CD**

a Data Destruction Register is to be completed when the DVDs are returned to Security and no longer required for evidential purposes.

b Details of all DVDs that fail to record, are to be recorded in the Data Destruction Register and then destroyed .

c No DVD is to leave the Control Room unless it is signed for.

d Score the disk with an abrasive; the disk should then be snapped/bent in half to prevent use.

2. SPOT TAPE/COPY TAPE

a Data Destruction Register is to be completed when the tapes are returned to Security and no longer required for evidential purposes.

b Details of all tapes that fail to record, are to be recorded in the Data Destruction Register and then destroyed.

c No tape may be removed from the Control Room unless signed for.

d Magnetically erase the tape. Pull tape from tape cassette and snap. If possible the tape cassette should also be damaged.

3. PRINTED MEDIA

a Data Destruction Register is to be completed when printed media (Images) are returned to Security and no longer required for evidential purposes.

b Details of all Still Images that are not required or are poor quality, are to be recorded in the Data Destruction Register and then destroyed.

c No Image is to leave the Control room unless it is signed for.

d All printed media (still images/reports etc) are to be destroyed by shredding.

Annex C-6

Sheet No……..

DATA DESTRUCTION REGISTER				
Ser	Date	Data Type/Serial No	Destroyed By	Signature

Annex C-7

Serial No

TEESSIDE UNIVERSITY SECURITY - VIEWING LOG - RECORDED MEDIA

System	**CCTV / INTERNAL** (Delete as appropriate)		
Building (Internal Only)		Digital Unit No/Spot Tape Ser No	
Camera Number(s)			
Reason for Viewing			
Outcome of Viewing			
Date		Viewed By		Signature	
Still Image(s) Produced	YES / NO	(If YES see Media Print Register for details)	

System	**CCTV / INTERNAL** (Delete as appropriate)		
Building (Internal Only)		Digital Unit No/ Spot Tape Ser No	
Camera Number(s)			
Reason for Viewing			
Outcome of Viewing			
Date		Viewed By		Signature	
Still Image(s) Produced	YES / NO	(If YES see Media Print Register for details)	

System	**CCTV / INTERNAL** (Delete as appropriate)		
Building (Internal Only)		Digital Unit No/ Spot Tape Ser No	
Camera Number(s)			
Reason for Viewing			
Outcome of Viewing			
Date		Viewed By		Signature	
Still Image(s) Produced	YES / NO	(If YES see Media Print Register for details)	

SECURITY CONTROL ROOM –EVACUATION PROCEDURE

In the event that the Security Control Room is to be evacuated in an emergency the following guidelines are to be followed by the Control Room Officer.

SHORT TERM EMERGENCY EVACUATION

1. Inform all radio call signs on Channels 1 & 2 that you are evacuating the control room.

2. Collect two (2) radios and the Emergency Log Book. This will maintain radio communications and a written record of events.

3. If time allows, secure all windows.

4. If time allows, log off desktop PC and switch off all monitors.

5. Leave control room ensuring the access control system engages to prevent unauthorised access.

LONG TERM EVACUATION

1. Inform all radio call signs on Channels 1 & 2 that you are evacuating the control room and moving to …(alternate location?) confirmed by Security Manager/Supervisor.

2. Transfer forward telephones to temporary Extn number.

3. Collect all available radios/chargers and the Emergency Log Book. This will maintain radio communications and a written record of events.

4. If time allows, secure all windows.

5. If time allows, log off desktop PC and switch off all monitors.

6. Leave control room ensuring the access control system engages to prevent unauthorised access.

In the event access is required to the Control Room by the Emergency Services, they should be accompanied by a Security Officer unless the situation is deemed too dangerous. If that is the case then the Emergency Services should be allowed unaccompanied access.

Annex E

Subject Access Request Form

The Data Protection Act 1998 gives individuals a right of access to their personal data which is held by the University. In order for us to process such a request, please complete and return this form to the address below. If you have any queries, please contact the University Secretary's Department by phone on 01642 342060 or by email to dpa@tees.ac.uk.

Data Protection Officer
University Secretary's Department
University of Teesside
Middlesbrough
TS1 3BA

If returning this form by hand, the University Secretary's Department is located on the second floor of the Student Centre. Working hours are 0830-1700 Monday to Thursday, and 0830-1630 Friday.

1. Details of the Data Subject *(ie the person who is the subject of the personal data)*

Full name: _____

Address: _____

_____

Telephone number: _____

Email address: _____

Relationship to the University (eg "current student" or "job applicant"): _____

Student number or staff payroll number (if applicable): _____

If you are a member of staff, do you mind being contacted by internal email/phone about this request? ❑ Yes ❑ No

2. Are you the data subject? ❑ Yes ❑ No

YES: If you are the data subject please supply evidence of your identity, eg a photocopy of your student card, staff card or driving licence.

NO: Are you acting on behalf of the data subject with their written authority? If so, that authority must be enclosed. We reserve the right to verify this directly with the data subject. If you do not have the subject's written authority, what other legal justification have you for seeking access to this data? Please note that identification as above must be provided for the requestor and the data subject.

Note that the University may request additional information to confirm the identity of the data subject and/or requestor as necessary.

3. Details of the requestor (if different from question 1)

Full name: _____

Address: _____

_____

Telephone number: _____

Email address: _____

4. Please describe the information that you are seeking, together with any other relevant information which will help us to identify the information you require. You should provide as much detail as possible. Attach an additional sheet if necessary.

5. The University is entitled to charge a fee of £10 for each data subject access request. However, access to all or part of one student or staff file may be charged at a reduced rate of £2. More comprehensive requests, and requests for supplementary information, will be charged at £10. Please enclose a cheque for either £2 or £10 payable to University of Teesside. Cash can be accepted if this form is returned by hand to University Secretary's Department. Please contact us if you are unclear how this applies to your request.

6. Declaration. To be completed by all applicants.

I confirm that the information given on this form is accurate and complete. I understand that it is necessary for the University to be satisfied as to the identity of the data subject and/or requestor, and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signature: _____

Date: _____

Please return the completed form to the address on the previous page. You must enclose:

- evidence of your identity
- evidence of the subject's identity (if different)
- authorisation from the data subject to act on their behalf (if applicable)
- the fee identified in question 5 above.

Annex F

TEESSIDE UNIVERSITY

Application to View Teesside University Security Cameras (Live Images only)

Title……. Forenames…….... Surname……..……..

School/Department…….…. Job Title……..……

Purpose and reason for requesting camera access……..……

……..……

……

Please supply details of Buildings and specific camera access (*Please list all locations*)

Building	Room Number or Location/Floor

Please read ALL of the following information carefully and sign below to signify that you have read and understood the conditions that apply to your access.

DISCLAIMER

I Confirm that all remote viewing will be kept confidential and NOT disclosed to a third party

SIGNATURE OF APPLICANT……

Print……..... Date……..
(Applicant)

Print / Sign…….…. Date……..……
(Dean / Assistant Dean / Director / Assistant Director of School/Department

BELOW THIS LINE FOR OFFICIAL USE ONLY

Print / Sign…….. Date…….

ACCESS TO VIEW

User Informed……Yes / No (delete as appropriate)

Document Control : CCTV Policy and Procedure	
Due for review by:	
Approved by:	EPC on 30 September 2011
Author:	Director of Campus Facilities
Department:	Campus Facilities Department