Security Policy

Owner:	Head of Security and Logistics
Reviewed by:	Estates Committee
Approved by:	Council (11 October 2010) Estates Committee (27 September 2010)
Review due date:	Currently under review
Update history:	

ROEHAMPTON UNIVERSITY
SECURITY POLICY

Appendices

INTRODUCTION

Roehampton University is situated in SW London and consists of seven separate sites The University is comprised of 64 buildings that are generally set within beautifully landscaped campuses within an average to below average crime area.*

There are approximately 8,000 students and 1000 staff at the University plus numerous visitors to the campus daily. There are staff car parking facilities at all campuses and car parking for students at Arton Wilson during term time.

Open access to University campuses are an essential ingredient of academic life but is not without risks. Some security measures are therefore necessary to maintain a safe and secure environment for our staff, students and visitors.

To increase the feeling and/or perception of security the University will develop and apply security controls, and procedures which will be widely published. Security is not intended to be a hindrance to academic activity. It is an essential ingredient for the safe and efficient operation of the University.

This Security Policy applies to all staff, students, visitors and contractors and seeks to formalise a cohesive and integrated approach to security throughout the University.

*Metropolitan Police

POLICY STATEMENT

The University will endeavour to ensure, as far as is reasonably practicable, the personal safety and security of all students, staff and visitors at all University campuses and University controlled buildings.

The Property and Facilities Management Department is responsible for the effective operation and enforcement of the Security Policy and Procedures.

Students, staff and visitors to the campus must also take responsibility for their security and personal safety. In particular, students, staff, visitors and contractors should assist the Security Service to ensure the success of the Policy.

Whilst minor breaches of the Policy may be dealt with informally, serious or repeated breaches will invoke disciplinary action.

Unless otherwise specified, reference to 'Roehampton University' in this document refers to Froebel, Digby Stuart, Southlands, Whitelands, Mount Clare Campuses, Downshire House and Arton Wilson.

RESPONSIBILITIES

Security Service will support the Security Policy by adopting a proactive approach to minimise crime and incidents and their effects on the University, staff and students. The Security Service will ensure the response to incidents is well managed by being responsive, effective and efficient. The Security Service will listen and care for our stakeholders and promote a safe and secure work and study environment

It is in the interest of the University that members of the University community report to the Security Service as promptly as possible any activity that appears to be criminal in nature.

Certain elements of these responsibilities fall to particular roles:

The Director of Property and Facilities Management will ensure that support and resources are available to the Security Service for the implementation of the Security Policy. Necessary measures to improve security in essential areas should receive priority consideration. Where appropriate, specific training to achieve acceptable standards of operation will be supported and properly resourced.

The Assistant Director Property and Facilities Management (Security, Fire and Transport) to be known as AD P&FM Security through this policy: will ensure overall development and planning of security strategy, policies and procedures and oversee the operation of the Security Service. Other responsibilities will include, but are not limited to the investigation of serious crime, breaches in security and advising on student disciplinary matters; provision of expert and impartial up-to-date advice, staff and student inductions, transport, liaison with police, emergency services and local authorities; management of the University fire detection systems, Security staff and CCTV systems; implementation of University Car Parking Policy.

Security Operations Manager will ensure the day-to-day management of the Security operation and monitoring of all policies and procedures to ensure their continued effectiveness.

Security Technical Manager will ensure the management of security IT systems, management and training of security staff in security access control issues; management & maintenance of CCTV and intruder alarm systems.

Senior Security Officers will ensure the day-to-day execution of the security policy and procedures; monitoring of these policies and procedures to ensure their continued effectiveness; delivery of an efficient and effective service to the University; management and training of staff; investigation of crime; reacting to University fire alarms.

Security Officers will deliver security duties as defined in job descriptions, including the patrolling of external areas to deter trespass and crime, daily

unlocking/locking of external doors through both electronic and manual processes. Follow procedures and access control for out of core hour events, responding to staff and student requests, first aid response, reacting to fire alarms and evacuation duties.

Heads of Academic and Non-academic Departments have a key role in promoting security within their area. It is recognised that Heads of Department may wish to delegate responsibility for the routine involved in these tasks to a nominated individual in their Department but the overall responsibility for security matters will remain with the Head of Department.

Staff: All staff must ensure and adhere to the University Security Policy, paying particular attention to those issues which are relevant to their activities. They must also co-operate with requests from the Security Service, especially in emergency or evacuation situations.

Students: They must follow security procedures designed to protect University property, in particular regulations governing access to computer rooms or areas with other public use equipment. Students must co-operate with requests from the Security Service, especially in emergency or evacuation situations and in relation to security procedures.

Student Invited Overnight Visitors (including family and friends) are the general responsibility of the host. The host should ensure the visitor(s) are guided to follow security procedures and policy designed to protect the University. The host is to book overnight visitors in and encouraged to ensure compliance, particularly in emergency situations.

General Visitors: (including conference delegates and external event attendees) have a general responsibility to look after the University facilities whilst on campus and to give due consideration to security issues. In particular they must follow security procedures designed to protect University property and where issued, carry their visitors pass at all times It is the responsibility of the host to ensure all visitors are informed and comply with the University Security Policy, particularly in emergency situations.

SECTION 1 – CRIME PREVENTION

1.1 SECURITY AWARENESS
Proactive crime prevention and security awareness will help to ensure a safe, secure environment, enabling work and study to continue with the minimum amount of disruption. Staff and students should make every effort to counter the threat of crime, as laid out in **Appendix A.**

1.2 INCIDENT REPORTING
Incident reporting is crucial to the identification of patterns of criminal activity. It permits investigation and recommendations to be made to prevent a recurrence. Comprehensive reporting of incidents provides an accurate picture of the level of crime throughout the University and thus ensures that adequate resources are provided to combat that crime which contributes to the success in the University's fight against crime. All incidents of a security nature should be reported and managed as laid out in **Appendix B.**

1.3 CRIME INVESTIGATION
All crimes that occur on University premises will be investigated appropriately to prevent re-occurrence and aid crime prevention. The AD P&FM Security or other members of the Security Service as delegated will carry out internal investigations of security related incidents, producing written reports for circulation where necessary.

SECTION 2- PERSONAL SECURITY

Whilst it is the responsibility of the Security Service to provide a safe and secure environment, it is the responsibility of all those on University premises to take all reasonable measures to ensure their own personal security.

2.1 STAFF AND STUDENTS
The Security Service will provide security briefs that staff and students are expected to attend during an induction period. Staff and students should be made aware of security advice publications and further advice as laid out at **Appendix G.**

2.2 CONTRACTORS AND VISITORS
All contractors who make use of and work on University property have a general responsibility to give due consideration to personal security issues. In particular they should follow security advice and procedures designed to protect them whilst on University property. A visitor's host or project manager has the responsibility to ensure security advice and procedures are made readily available.

SECTION 3 – ACCESS & IDENTITY CONTROL

3.1 IDENTIFY CARDS
All staff and students are issued with a Roehampton University card which is used as an identity card, access card and a Library membership card. **The card is non-transferable and may only be carried and used by the individual to whom it was issued.** Staff and students should carry their card with them at all times when on University property and must show their card to Security Staff on request. Loss of identity cards must be reported to security as soon as possible. Overnight visitors, long term visitors (beyond five continuous working days) and contractors will be issued with a 'security visitor's pass at any Security Reception location which must be carried at all times while on University property **(see Appendix C).** Security will reserve the right to establish the identities of all persons on Roehampton University estate and detain any issued identity card or pass following an incident on campus. Roehampton University identity cards will be forwarded to an SWO for student issues and retained by the AD Security for staff, visitor and contractor issues and reissued via departments if deemed appropriate.

3.2 ACCESS CONTROL
Access Control Systems operate in some areas. Card controlled barriers/doors are an effective method of preventing unauthorised access and the security strategy will move towards expansion of access control systems throughout the University. Access cards will be regarded for security purposes the same as a key. Cardholders must safeguard their card and report any loss to the Security team as soon as possible **(See Appendix C).**

3.3 UNIVERSITY CORE HOURS
Core hours are defined as Monday to Friday 8 a.m. to 9 p.m. excluding public holidays. If work needs to be done or continued outside those hours and you feel at risk, the Security Service should be informed.

Access to the University outside core hours will be in accordance with the process set out in the lone working policy. **(Appendix C).**

3.4 CONTROL OF LOCKS & KEYS
Any requests for locks and keys for new premises, refurbishments and replacements will be in consultation with AD P&FM Security.

Security carries out duties over 24hrs, 365 days per year and requires access to all areas especially in emergency situations. Any request made by Security for keys (or access to keys) codes; swipe cards; any others means of access, must be granted in order that emergencies can be dealt with immediately. In exceptional circumstances certain restrictions may apply to sensitive areas (research) but agreement will be achieved between interested parties regarding access in any emergency situation. **(see Appendix D).**

SECTION 4 – PROTECTION: EQUIPMENT/ DOCUMENTATION

4.1 SECURITY OF EQUIPMENT
The safekeeping of all property will help to ensure that the maximum amount of equipment is available for use at all times. Students and staff are to make all possible effort to ensure that all equipment is protected from the possibility of theft or damage as described at **Appendix E.**

4.2 SECURITY HARDWARE
Installation of CCTV, intruder alarms or access control systems on University property will only be undertaken following consultation with AD P&FM Security who will advise on equipment, installers and security response. Where CCTV is installed, the requirements of the University's Data Protection Policy and of the Data Protection Act must be adhered to.

4.3 HEADED PAPER AND STATIONERY
Pre-printed headed paper and other stationery displaying the University logo, staff names and telephone numbers should be locked away when not in use.

4.4 DATA PROTECTION
The data of living persons is protected under the Data Protection Act www.ico.gov.uk. The Act creates responsibilities and rights in relation to all aspects of the collection, holding, use and disposal of personal data. Staff should handle personal data in accordance with the University's Data Protection Policy and the Data Protection Act. Staff should ensure that they are aware of University policy in this area and of the sources for further advice. Information relating to the DPA 1998, training materials, and sources of information are published on the Intranet to which all students and staff have access.

4.5 PROTECTING INFORMATION ASSETS
Maintaining the security of computers and related equipment is vital to the University. Computers are prime targets for theft; they are easily disposed of and have a high value. The theft of a computer may also lead to delays in University processes, the loss of important data and disruption to learning and teaching. Viruses and worms damage software and data; result in time lost and can close down whole organisations.

Damage of this type is not inevitable and by being aware of simple security measures and observing them, the chances of loss and damage can be minimised. Information on how to protect data and the equipment on which the data is processed is available on the Information Services and Systems site. IT and AV equipment users should access the site and employ the guidelines available as per the University IT policy.

4.6 CONFIDENTIAL WASTE
It is the responsibility of the Departments requesting disposal through Property and Facilities Management to ensure confidential material is secured at all times until collected.

SECTION 5 – ASSET PROTECTION

5.1 CONTROL OF CASH
Security discourage the storage of any large amount of cash (£50 or over) on University premises outside appropriate secure rooms. Cash kept on University premises must be held in accordance with the University's Finance Policy.

5.2 SECURITY OF ACADEMIC BUILDINGS
It is the responsibility of the Security Service to secure the external entrance/exit door to each academic building outside core hours. This will be through electronic or manual methods.

5.3 SECURITY IN THE OFFICE
It is the responsibility of all staff to secure their own office space as laid out at **Appendix F.**

5.5 DRUGS AND ILLEGAL SUBSTANCES
All suspicions of the handling or using of controlled or illegal substances should be reported to the AD P&FM Security in the first instance, so that appropriate investigation and consultation with University authorities may take place. Policy and guidelines on the misuse of illegal drugs is set out at www.roehampton.ac.uk/about/policies/DrugsPolicy.pdf. Departments which hold substances that might constitute a security or safety risk should contact the Manager, Health and Safety or the AD P&FM Security for advice on best practice.

5.6 PROPERTY LOST AND FOUND
All lost and found property should be handed in to the Security Service at Security Reception, Digby Stuart. When property is handed in, the date/time, finder's name, department and contact details will be recorded. If the property is not returned to the owner or left unclaimed for more than 3 months, the property will be destroyed. A guide to dealing with lost and found property is at **Appendix I.**

SECTION 6 – PARKING (cars, motorcycles, bicycles)

6.1 PARKING
Parking on University property, including the parking of motorcycles and bicycles, will only take place in recognised parking locations and requires an appropriate permit to be displayed. A guide to parking and permit requirements is laid out at **Appendix H.**

The University does not accept any liability for vehicles, motorcycles, scooters or bicycles or their contents when parked or left on University premises

SECTION 7 - USE OF CLOSED CIRCUIT TELEVISION (CCTV)

7.1 REASONS FOR USE
CCTV is recognised as a powerful tool in the fight against crime, both for prevention and detection. The University uses CCTV systems around the campus covering many of the vulnerable areas, public access points and adjacent streets.

CCTV

- May reduce the fear of crime and offers public reassurance for students, staff and visitors to the campus.
- Can assist in the detection, deterrence and prevention of crime on campus by securing evidence to identify, apprehend and prosecute offenders and to provide evidence for internal disciplinary hearings.
- Appropriate signs will be placed around the University warning that CCTV is in use. The University's CCTV Code of Practise is available on the Security website.

7.2 LOCATIONS
The University CCTV system consists of both internal and externally located overt cameras with telemetry and digital recording. It is agreed that some departments may benefit from a local CCTV system for the reasons described above. The operation of these systems and any future installations in departmental areas, must be authorised by the AD P&FM Security and comply with the Data Protection Act (DPA).

7.3 CCTV OPERATING PROCEDURES
It is intended that the information obtained from CCTV will give public confidence that the rights of individuals are being fully protected and the requirements of DPA are complied with.

Access to the CCTV monitoring and recording systems is strictly controlled and is limited to duty security staff or authorised management.

7.4 THE POLICE (GENERAL) AND CCTV
It is recognised that the Police in the course of their duties may have reason to enter the Roehampton University estate. This can be as a result of immediate follow up to an incident, search of premises, being invited to assist the Security Service or post incident investigation.

The Police (where practically possible) should always inform security they intend to work on the Roehampton University estate in emergency situations and immediate incident follow up. Security staff should always remain with the Police whilst on the Roehampton University estate in such a situation. If Security Officers are asked to leave the area by the Police they should remain within the vicinity and ensure AD P&FM Security is informed.

Security Officers in attendance would not be applicable for pre-arranged visits or appointments.

Police asking to enter student accommodation will be asked by Security Service to produce a warrant, if a warrant cannot be produced then the AD P&FM Security should be informed. Security staff will not automatically allow access before obtaining clearance.

Police should not require access to (nor be allowed access to) University CCTV systems except under the following circumstances:

Emergencies or investigation of serious incidents
Identification of offenders
Liaison and training purposes, by prior arrangement with the Head of Security
As authorised by the AD P&FM Security.

Requests by Police to remove CCTV recordings must comply with the DPA and will be registered accordingly.

7.5 RECORDED IMAGES
CCTV Images will be kept securely and in line with the requirements of the Data Protection Act.

7.6 COVERT CCTV
Covert CCTV will not generally be used within the University but may be used in exceptional circumstances to assist in the detection of crime or apprehension of offenders. Before use, permission to use covert CCTV will be obtained through the Director of P&FM, HR and University Secretary. It will be sited only for a time specific and necessary to the operation. Recordings from covert CCTV will be treated in accordance with the Data Protection Act.

Appendix A

CRIME PREVENTION

- All suspicious activity should be immediately reported.

- Personal valuables will be locked away or placed out of sight or kept on the person, and personal property will never be left unattended.

- Windows in ground floor offices must be closed and secured on departure where locks are fitted. Curtains or blinds in these rooms should be closed at dusk and lights (except security lighting) should be turned off when leaving.

- Laptops and other portable IT/AV equipment will be locked out of sight when not in use, particularly overnight, in open areas.

Appendix B

<u>INCIDENT REPORTING</u>

- All security incidents should be reported to Security Reception at Digby Stuart Gate House on ext 3140 (24 hours) or ext 3333 in an emergency.

- All reported incidents will generate an incident report and will be forwarded to AD P&FM (Security) who will forward for appropriate action.

- All suspected criminal offences will be reported to the Police.

- All emergency Police involvement on any campus is to be notified to the AD P&FM Security to enable effective University management of any subsequent actions on University premises.

- Security Services should be informed as soon as possible when emergency services are requested to Roehampton University.

- Suspicious behaviour – Staff, students and visitors should not place themselves in a vulnerable or confrontational situation if they observe suspicious behaviour. More important is to make a mental or written note of a description, direction of travel, what suspicious acts have been witnessed and any other information which may help Security identify and locate the individual(s). That information should be provided to Security as soon as reasonably possible. Each situation of this type will be different and it is at the discretion of the individuals concerned as to what action they wish to take, but at no time should they put themselves at risk.

.

Appendix C

<u>ACCESS CONTROL</u>

- Long term visitors (beyond five continuous working days) and Contractors will be issued with a 'security visitor's pass' at Security Reception, Digby Stuart. The member of staff or student responsible for the long-term visitor/contractor will ensure that the visitor/contractor collects or return the pass when signing in or out of the University.

- Contractors on site for more than a week (five days) will be issued with a University 'Contractor' pass. Arrangements for these cards are to be agreed in advance by the Contract Project Manager and AD Security. The Contractor pass must be displayed at all times whilst on University premises.

CONTROL OF LOCKS & KEYS

Staff

- All applications for new barrels or keys should be made via a footprints request to the P&FM Department Helpdesk.

- All issues of keys by Security will be subject to satisfactory fulfilment of criteria to ensure need, use and availability.

Contractors
Contractors' access to University buildings will be strictly controlled by the Security Service according to agreed access control procedures

Student Room Keys
Student room keys are the responsibility of the student to whom they were issued and may not be transferred or used by anyone other than the person who signed for them.

General

- All losses of staff keys must be reported immediately to the Security Service.

- Persons leaving the University are to return their keys direct to the issuer as appropriate. They should not pass keys directly to their replacement.

- Any loss of master or sub-master keys will be the subject of an inquiry. If loss of master or sub master keys is suspected to have arisen through negligent action by a member of staff, then an investigation under the appropriate Disciplinary Procedure should be undertaken. Further disciplinary action may be taken if appropriate, following the completion of the investigation.

Appendix E

SECURITY OF EQUIPMENT

All computer/AV equipment should be secured dependent on its use.

The physical protection of IT and AV equipment is important on and off campus. Equipment used in departments must be managed to reduce the risk of the equipment being damaged, stolen or accessed by unauthorised persons.

- All valuable portable IT and AV equipment such as laptops & PDA's, must be locked away out of sight when not in use, especially overnight.

- All valuable equipment should be marked using the appropriate identification method (i.e. UV pen, Smartwater etc). Advice on this can be sought from the Security Service.

- Suspected thefts of equipment should be reported promptly to the AD P&FM Security.

- Heads of Departments are responsible for maintaining inventories for all equipment and furniture in their departments.

Appendix F

SECURITY IN THE OFFICE

At the end of the working day, staff should ensure that:

- Valuables and confidential documents (laptops, exam scripts, research data, personnel files etc) are locked away with keys secured in key cabinets or taken home:

- Any departmental keys that have been issued during the day have been returned and any losses reported immediately.

- A 'clear desk policy' is maintained where possible to ensure confidential documentation is locked out of sight.

- Doors and windows are closed and locked as appropriate.

- Ground floor curtains and blinds are closed with any items on windowsills, which hinder closure, removed and lights turned off.

- Intruder alarms (where installed and a local responsibility) are set.

- PCs are switched off or password protected when not in use to prevent unauthorised access to information.

Appendix G

<u>PERSONAL SECURITY</u>

Staff, students and visitors should try to avoid walking on their own in the dark and should familiarise themselves with any late night transport arrangements provided. Keep to well-lit and busy streets, avoid pedestrian underpasses, and use designated safe walking routes where available.

Be aware of people when using a cash machine and preferably draw out money during the day.

Do be suspicious of e-mails or phone calls requesting too much personal information and destroy papers carrying bank or credit card details. Identity theft is on the increase.

Keep a record somewhere safe of plastic card details and the serial and model numbers of your expensive electrical equipment.

Mark your possessions with a UV pen.

Do try to avoid using your mobile in isolated places.

Texting can distract you from what is happening around you. When you are out and about switch your mobile to vibrate mode rather than a ring tone.

Consider installing security software on your laptop and always carry it hidden inside a sports bag rather than in its own obvious case.

Immobilise your car or lock your bike whenever you leave it even for a few minutes.

Moving between University buildings - students and staff should make themselves aware of their surroundings and of other people when walking between buildings. Try to avoid poorly lit or isolated areas and where possible, walk with other members of staff or students. Report any deficiencies in lighting on University buildings through the P&FM Helpdesk so that remedial action can be taken where appropriate.

Reporting suspicious activity is extremely important to Security Staff in helping to prevent and detect crime against the University.

If staff or students are faced with threatening or abusive behaviour, stay calm, avoid raising your voice and the use aggressive body language such as finger pointing/wagging. Call for assistance from colleagues and/or Security Staff.

Appendix H

PARKING

Car Parking Staff

Parking is available to staff on application and all cars must display a valid Roehampton University parking permit issued by security. Available on-line.

Car Parking For Students With Mobility Limitations On A Temporary Or Permanent Basis

Parking for students with mobility limitations on a temporary or permanent basis is available. Cars will display appropriate blue badge or Roehampton University permit available on-line. All applications for this type of pass will be via the appropriate SWO.

Student Parking During Core Hours 0800-2100hrs

No parking is offered to students at Digby Stuart, Froebel, Southlands, Whitelands, Downshire House and Mount Clare from **0800-1630hrs.** The 1630hrs start time will reduce local off street parking requirements.

Limited parking is available to students at the Arton Wilson car park during term time on a "first come first serve basis". All student car owners must apply and display a valid permit available on-line

Student Weekend Parking

Students may park at Digby Stuart, Froebel, Southlands, Whitelands and Mount Clare from Friday 1630hrs through to Monday 0800hrs. A visitor permit is required from Security Reception, Digby Stuart.

Student Parking Non Term Time

During non term time students may park on the University sites in recognised bays. Car owners must display a visitor pass available from Security reception, Digby Stuart.

Overnight Student Parking

Overnight parking is available from 1630hrs – 0800hrs Monday to Friday. Student owned cars must be removed by 0800hrs. Car owners will display a visitor pass available from Security reception, Digby Stuart.

- *Digby Stuart Gates close at 2300hrs and reopen at 0600hrs. The gate will only open for emergency service vehicles between these times.
- Froebel gate closes at 1900hrs and can only be accessed with appropriate access rights.

Visitor Parking

Visitor parking is available (but limited) on all sites. It is the responsibility of the member of staff issuing the invitation to make the necessary arrangements. Where possible, visitors should be encouraged to use public transport and the University Shuttle Bus between campuses.

Contractor Parking

It is the responsibility of the member of staff leading a project to make the necessary arrangements with the AD P&FM Security and Fire for the issue of a permit. This should be arranged at pre contract meeting by project managers and limited to a max of two 2 parking permits.

Enforcement

Drivers of Vehicles parked in breach of the Car Parking Policy are liable to receive a penalty notice.

Cars parked for more than 48 hours without prior notice may receive a penalty notice and removal from the University estate.

Cycle Parking

Anyone leaving a bicycle on University premises should be aware of the importance of having a robust lock and knowing how to use it effectively and having it insured.

All cycles owners will register their bicycles on-line with security and display a valid permit issued security.

Non registered cycles locked in one location for more than a two week period without prior notice will have the cycle removed. This will occur after a period of not less than seven days notice on the cycle informing of the security intention to remove.

Motorcycle Parking

All motorcycle owners will register their motorcycles on-line with security and display a valid permit issued by security.

Anyone leaving a motorcycle or scooter on University premises must leave it safely and securely locked. All motorcycles must display a valid permit available from security. Applications should be submitted through the security website.

Appendix I

PROPERTY LOST AND FOUND

Lost and Found Property

All University lost and found property will be logged by Security Reception and then collected and stored by AD P&FM Security as soon as practical.

All unclaimed articles will be held for a minimum of 90 days. After 90 days all articles will be destroyed. Found cash will be donated via local charity boxes. Articles of a personal nature such as credit cards or driver's licenses will be destroyed (shredded) and disposed of in a non-compromising manner.

Destruction of items will be recorded by AD P&FM Security and counter signed by another AD P&FM.

Any person(s) reclaiming items will need to offer a full description and evidence that the item to be reclaimed is their property. All reclaimed must be signed for.

The finder of lost property must advise Security if they intend to claim the property if the rightful owner does not.

Equality impact assessment
School/Directorate: Roehampton University

Name of person completing the equality impact assessment:

Paul Markham-James

Date of completion: 10 Jane 2010

What is the name of policy / function / practice / criteria you are equality impact assessing? Security Policy

Is the policy:

New   ☒
Existing   ☐

Screening
What is the aim of this policy / function / practice / criteria? What is it intended to achieve?

Policy- The aim of the Security Policy is to equip Roehampton University with the nessacary processes to ensure the service provides a safe and secure environment.
Who are the main stakeholders?

Staff   ☒
Students   ☒
Community ☒

In light of the data and evidence you have collected for this equality impact assessment, does this policy / function / practice / criteria have any relevance to, or impact on, equality and diversity in the two areas below?

Possibility for discrimination / adverse impact   ☐
Opportunities to promote equal opportunities / good relations   ☒

Evidence and data
Please use the space below to discuss the evidence and data you have collected for this equality impact assessment. *This evidence may include statistics, results of consultations, feedback, external reports etc. There is no set format for this section; please include any information that is relevant or that you have collected which you have considered as part of this equality impact assessment. Discuss how it has enabled you to make your conclusions about any impacts on equality of what you are assessing.*

Please ensure you include feedback where appropriate on the policy / function / practice / criteria from the three staff forums: Race Equality, Respect Sexual Orientation, and N-Able Disabled Staff Group. You can obtain further guidance and details on the staff forums from the Equality Unit.

In assessing the security policy, my findings does not indicate any differential impact, nor is there really any way that the policy might affect different groups in different ways.

Equality impact

Based on your findings presented in the section above, please tick the appropriate boxes below and summarise your reasons where appropriate:

	Positive impact/ opportunities	Negative / adverse impact	No impact	Unknown	Reasons and evidence
Race	☐	☐	☒	☐	
Gender	☐	☐	☒	☐	
Disability	☐	☐	☒	☐	
Sexual orientation	☐	☐	☒	☐	
Religion or belief	☐	☐	☒	☐	
Age	☐	☐	☒	☐	

If you have identified any negative or adverse impact, can this be justified?

Yes ☐
No ☐

If you have answered yes, please explain how:

What action will you take to reduce the negative or adverse impacts?

Changes to the policy / function / practice / criteria ☐
Changes to the method of implementation ☐
Replacing the policy / function / practice / criteria ☐

Please discuss further:

Action planning:

Action required	By whom	Date for completion

Publicising and reporting
The Equality Unit will work with you to ensure this equality impact assessment is adapted for publication on the University website.

Please use the space below to discuss how else you want to make the results of this equality impact assessment more widely known. This might include presenting it at School or Directorate forums, committee meetings etc, or sending it to those who were consulted; you may have your own internal channels of communication you want to use.

Monitoring and review
When will you review this equality impact assessment?

On policy review
Who will be responsible for the review?

Head of Security
How will you monitor the policy / function / practice / criteria in the meantime?

This might include collecting periodic feedback, checking statistics periodically etc. There is no requirement for another full equality impact assessment at this stage.

Through customer surveys and feedback if any new information has come to light which indicates changes are needed to eliminate any unlawful discrimination then the policy will be amended.
Approval
Dean / Director of School / Director signature:

Date: 10 June 2010

Date sent to Equality Unit: