



London School of Economics & Political Science

Physical Security Policy

Final Draft:	06/11/12
Approved by Estates Strategy Committee:	22/05/13
Next Review Date:	22/05/14

London School of Economics Physical Security Policy

The purpose of this policy is to provide a framework and procedures for identifying and dealing security risks facing LSE, its staff, students and visitors

1. INTRODUCTION	2
2. ROLES AND RESPONSIBILITIES	3
3. CAMPUS SECURITY	5
4. RESIDENCES SECURITY	6
5. CRIME PREVENTION	6
6. PUBLIC EVENTS	8
7. ASSET PROTECTION	8
8. CONTROL OF LOCKS AND KEYS	9
9. EMERGENCIES	10
10. SECURITY SAFETY PROCEDURES	11
11. POLICY REVIEW	11

APPENDICES

Appendix A: General Information	12
Appendix B: Security Risk Analysis Principles	14
Appendix C: Crime Prevention and Security Awareness	15
Appendix D: Personal Safety	16
Appendix E: Lost Property	17
Appendix F: Control of Locks and keys	18
Appendix G: Handling Bomb or Suspect Material	19
Appendix H: Security Safety Policy	20
Appendix I: Security Operational Procedures	21

Produced by: PT HoS/AB DFM: 22/10/2012

Checked by JSR Director of Estates: 31/10/2012

1. INTRODUCTION

The London School of Economics and Political Science (hereafter referred to as LSE) main campus is situated in central London. The main campus

has 28 buildings. There are also 12 halls of residences situated around central London and the Sportsground. There are approximately 9,000 full time students and a staff complement of just over 3,000, as well as a large number of visitors who come to the School daily.

The purpose of this policy is to provide a framework and procedures for identifying and dealing with security risk facing LSE, its staff, students and visitors. This policy will allow the School, in as far as is reasonably practicable, to ensure the safety and security of the campus, outlying facilities (i.e. residences) and the people using these facilities.

The Policy:

- Defines the roles and responsibilities of relevant persons
- Confirms LSE's determination to minimise the security related risk facing the School.
- Affirms LSE's commitment to have in place security systems, procedures and control measures that ensure that the LSE community, including visitors to the School, can go about their business in a safe and secure environment.

2. ROLES AND RESPONSIBILITIES

2.1 Management and Responsibilities

It is essential that adequate resources are made available for managing the risk arising from security related issues within the School. It is important that all personnel involved in implementing this policy are competent, trained and aware of their responsibilities.

2.2 Director of Estates

The Director of Estates is responsible for all strategic aspects of security across the School's properties.

2.3 Director of Facilities Management

The Director of Facilities Management will ensure that support/training and resources are available to the Security Team to implement the Security Policy, including assembling and maintaining a suitably qualified security team.

2.4 Head of Security

The Head of Security will be responsible for the development of strategic security, drafting the LSE Security Policy, and will take the lead role in its

implementation and will propose amendments to the Security Policy that may be necessary in the future.

2.5 Security Operations Manager

The Security Operations Manager will manage the day to day implementation of the Security Policy and monitor its continued effectiveness.

2.6 Security Team Leaders

Security Team Leaders will be responsible for the day-to-day organisation and supervision of security officers as defined in the operational procedures.

See Appendix I: Security Operational Procedures

2.7 Security Staff

Security staff will carry out duties as defined in the operational procedures.

See appendix I: Security Operational Procedures

2.8 Heads of Departments/Divisions

Heads of Departments/Divisions, supported by the Security Department, are responsible for security within their areas.

2.9 Staff

All staff must be knowledgeable of and adhere to the Security Policy.

2.10 Students

Students must follow security procedures and co-operate with requests from the Security Team and SU Events Security, especially in emergency or evacuation situations.

2.11 Visitors

Visitors are required to follow LSE's security procedures and follow directions from their host or the Security Team or section, particularly in an emergency situation. Where issued, visitors must display their pass at all times. It is the responsibility of the host to ensure all visitors are informed of and comply with the LSE Security Policy.

3. CAMPUS SECURITY

The Security Team operates a number of security systems in order to keep the School premises and surrounding environs safe and secure for staff, students and visitors.

3.1 Closed circuit television (CCTV)

LSE uses CCTV systems around the campus (outside and inside buildings) covering many of the vulnerable areas, public access points and adjacent streets. The CCTV system and all its recordings are owned by LSE and the system is operated by the School's Security Team.

3.2 Purpose of CCTV

The LSE Security Team uses CCTV to protect life and property and to prevent crime. It is used for no other purpose. The images captured are recorded and retained in the event that they may be needed as evidence of criminal activity.

3.3 Privacy and Disclosure of Images

All images from the CCTV system are treated in accordance with the Data Protection Act of 1998. Under the Data Protection Act individuals, who have been monitored by a CCTV system, have a right of access to their recorded images. Requests to access recorded images must be made to the Head of Security. Further Information on the Data Protection Act and the School's policy can be found here:

<http://www2.lse.ac.uk/aboutLSE/dataProtection/Home.aspx>

3.4 Covert Cameras

Covert cameras are not in general use around the campus. However, on occasion it may be necessary to operate such cameras for the purposes of detecting crime and/or apprehension of offenders. Before use, permission to use covert cameras will be obtained through the head of the relevant department or division. It will be sited only for a specific time period and as necessary to the operation. Recordings from covert CCTV cameras will be treated in accordance with The Data Protection Act of 1998.

3.5 Alarms

The Security Team operates a number of perimeter breach, intruder and panic alarms which are monitored 24/7/365 from the Security Control Room. Security will respond immediately to the activation of these alarms.

3.6 Security Patrols

Members of the Security Team will carry out regular overt patrols of the buildings and campus environs in order to provide a visible deterrence to criminal activity. They will also carry out covert operations as part of the efforts to keep the campus crime free.

4. RESIDENCES SECURITY

Residences security is currently under review and will be included at next update.

5. CRIME PREVENTION

5.1 Security Risk Analysis

All departments and divisions will be responsible for assessing and mitigating security related risk arising from their activities. In liaison with the Security Team, departments and divisions should carry out periodic risk assessments to determine their security needs.

See Appendix B: Security Risk Analysis Principles

5.2 Security Awareness and Reporting of Incidents

All persons on campus or in the halls of residence must report any incident of crime and suspicious activity (even if not of a criminal nature) or items to the Security Team immediately. The Security Team will always treat any reports seriously and respond accordingly.

Departments or individuals responsible for an activity that may impact on the security of the campus or the halls of residence must also report this to the Security Team.

See Appendix C: Crime Prevention and Security Awareness

5.3 Personal Security

The LSE is an open campus and this provides for a free and collegiate atmosphere that many in the School enjoy. Whilst it is the responsibility of the Security Team to provide a safe and secure environment, it is the responsibility of all to take all reasonable measures to ensure their own personal security.

5.4 Staff and Students

The Security Team will provide security briefs to staff during their induction period. Academic heads of departments are responsible for providing this brief to students during their induction. Further tips on personal security can be found in Appendix D: Personal Safety.

5.5 Contractors and Visitors

All contractors who make use of and work on LSE 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 LSE property. A visitor's host or project manager has the responsibility to ensure security advice and procedures are made readily available.

5.6 ACCESS CONTROL

5.7 LSE Identity Cards

All staff and students will be issued with an LSE ID Card. This card acts as an identity card, a library member card, a student registration card and an access control card. Cardholders must safeguard their card and report lost cards as soon as possible. Identity cards are not transferable nor should they be loaned out to anyone for any purpose. The identity card remains the property of LSE.

5.8 Enhanced Access Levels (Staff Only)

Initially the LSE ID card is issued with basic level access. Staff members, who require more developed access, need to have written authority from their head of department. Only then will the Security Team encode the ID card to reflect the desired access level.

5.9 Lost Cards

All lost LSE ID cards must be reported to the relevant issuer immediately to prevent misuse by unauthorised individuals.

5.10 Students

Students must report lost cards to the Student Services Centre (SSC) as soon as possible. Procedures for reporting a lost card can be found at:

<http://www2.lse.ac.uk/intranet/students/campusLondonLife/studentIDCard.aspx>

5.11 Staff

Staff must report lost cards to the library as soon as possible.

6. PUBLIC EVENTS

Public events are defined as an event where over 30 members of the general public may attend. The School's policy on public events is contained in the administrative notes to the School Code of Practice on Free Speech which can be found here:

<http://www2.lse.ac.uk/intranet/staff/SchoolRegulations/codeOfPracticeOnFreeSpeech.aspx>

For the organising entity, the following security and access control considerations must be observed:

6.1 Security

- The organising entity must ensure that they complete the public events security questionnaire and forward this to LSE Conferences and Events. The security questionnaire can be found here:
- <http://www2.lse.ac.uk/intranet/LSEServices/ERD/conferenceAndEventsOffice/information/riskassessment.aspx>
- In some cases a full security risk assessment may be recommended by Conferences and Events. The organising entity must liaise with the Security Team in the commission of this risk assessment.
- In certain cases the provision of enhanced security may be recommended as a result of the risk assessment.

6.2 Access Control

Members of the public are permitted to be on the School premises for the duration of the public event they are attending. Most events are on a first come first served basis but some are ticketed and access is granted only to those with a valid event ticket.

7. ASSET PROTECTION

It is the responsibility of all staff and students to take reasonable measures in protecting School property, as well as their own personal property, from theft or damage.

7.1 Control of Cash

Members of staff who handle cash on behalf of the school must adhere to the cash handling guidelines provided by the Finance Division.

7.2 Security of Buildings

The Security Team is responsible for the securing of all external entrance/exits doors to all buildings outside the School's main operating hours. It is the responsibility of all staff to secure their own office space.

7.3 School Equipment

Staff and students are to make all possible effort to ensure that all School equipment is protected from the possibility of theft or damage. Staff members have a special responsibility to take appropriate measures to ensure that equipment directly under their control is kept safe and secure. Members of staff are expected to seek advice from the Security Team.

7.4 Personal Property

It is the responsibility of everyone to take reasonable measures in ensuring that their personal property is safe. The School offers secure parking for bicycle as well as secure storage for laptops. Further details for this and other tips to keep your personal property safe can be found in Appendix D: Personal Safety

7.5 Lost Property

Any lost and found property should be handed in at the reception desks of the Old Building, the New Academic Building and the Library. A guide to dealing with lost and found property is found in Appendix E: Lost Property.

8. CONTROL OF LOCKS AND KEYS

Keys are issued via the School Estates Division. New issue of locking systems or keys can only be requested by a departmental administrator. This request should be done via the LSE Estates replacement/additional lock request form which can be found at:

http://www2.lse.ac.uk/intranet/LSEServices/estatesDivision/HelpdeskAndServices/serviceRequesthelpdesk/serviceRequest_additionalOrReplacementLocks.aspx

Guidelines for this can be found in Appendix F: Control of Locks and keys

9. EMERGENCIES

Staff and students are encouraged to familiarise themselves with the information provided by the School on what to do in an emergency. They should also familiarise themselves with the contact details for the Security Team, the police and other emergency services. More details on what to do in an emergency can be found at:

<http://www2.lse.ac.uk/intranet/news/businessContinuity/home.aspx>

9.1 *Major Incidents*

The Major incident Initial Response Plan (MIIRP) sets out the framework for the actions to be taken at School level in response to the early stages of a major incident affecting the Houghton St campus or a student residence. The objective of the plan is to help ensure the safety and wellbeing of people and security of property in the immediate aftermath of the incident. Further details on MIIRP can be found at:

<http://www2.lse.ac.uk/intranet/news/businessContinuity/aboutBusinessContinuity.aspx>

9.2 *Fire Alarm Activations*

In the event of a fire alarm activation the Security Team is responsible for managing the incident, including managing an orderly evacuation of the building and directing occupants to the designated fire assembly point, and calling the Fire Brigade if necessary. Under no circumstances can anyone re-enter the affected building(s) without the all clear and go ahead from the Security Team or the Fire Brigade.

Staff, students and visitors to the School are required to cooperate fully with security officials in the event of fire alarm activation.

9.3 *First-aid*

If a person has an accident or is taken ill please dial 666 to summon first-aid assistance. The Security Control Room will have lists of first-aiders on campus and the location of first-aid supplies. They will also summon an ambulance if it is required.

9.4 *Bomb and Suspect Material*

Any member of staff or student who receives a suspicious package should not open the package, but immediately call security on 666. Members of staff, students and visitors are encouraged to report any suspicious items such as bags left unattended to security. Security will respond to all calls and take appropriate action. Further details on the

course of action to take are found in Appendix G: Handling Bomb or Suspect Material

9.5 Contacts

9.5.1 The Security control Room

The Security control room is staffed 24 hours a day every day and can be contacted on the following numbers:

Emergency Line: 666 (Internal) or 020 7955 6555

General enquiries: 2000 (Internal) or 020 7955 6200

9.5.2 Contacting the Police Fire and Ambulance

The emergency services number is 101.

10. SECURITY SAFETY PROCEDURES

Recognising means that the risk (physical, legal and reputational) inherent in security operations means that risk assessment must be carried out on the basis of complete information. Many and varied factors can impact on security risk assessment and the responsibility to identify these factors rests with the Security Team Management Team.

All departments and divisions within the school are responsible for the full disclosure of information as required by the Security Team for the purposes of security risk assessment. For further details see Appendix H: Security Safety Procedure.

11. Policy Review

This policy will be reviewed annually, or as new knowledge on the subject evolves and subsequent guidance is issued.

Appendix A: General Information

School's Main Operating Hours

Monday - Friday: 09:30 – 19:00

Security will begin to lock down the campus buildings at 18:30

During weekends, including bank holidays and School closure periods, School buildings are closed for general use. Notices advising of access during bank holidays and closure periods will be posted to all students and staff when appropriate.

After Hours Access

Staff and students will be able to access the main School buildings up till 10pm or midnight, depending on the building in question. Production of a valid LSE identity card will be required before entry is granted. Entry after hours is via the Old Building only.

Members of staff who require access to their offices outside normal working hours and weekends will require written authorisation from their heads of department before the Security Team can encode their LSE staff identity cards to give them the required access.

Library Operating Hours

Michaelmas Term

Monday – Sunday: 08:00 – 00:00

Lent and Summer Terms

The library is open 24hrs a day

Visitor access to the library is only until midnight. Library staff will carry out patrols to ensure that only LSE staff and students are in the library after midnight.

Staffed Services

Monday – Friday: 09:00 – 20:00

Saturday and Sunday: 11:00 – 18:00

Public Holidays and Closure Periods

Notices of opening arrangements during public holidays and School closure periods will be made available by the library and published on the LSE Library website.

Gym and Other Sporting Facilities

Monday – Friday: 08:00 – 21:00

Saturday: 10:00 – 18:00

Sunday: 11:00 – 17:00

The gym and other sporting facilities are closed during public holidays and School closure periods. Non LSE users of sporting facilities are required to show a membership card.

Alumni Access

Monday – Friday: 08:00 – 18:30

More details can be found at:

<http://www.alumni.lse.ac.uk/olc/pub/LHE/filemanager/help/access.htm>

Visitors

Visitors and contractors to the School are required to present themselves to the reception desks where they will be issued with a visitor or contractor pass authorising them to be on LSE premises. The visitor or contractor must display their pass at all times during their time at the School and return it to the point of issue at the end of their visit.

Maintenance Visitors

In addition to 6.6 above, maintenance visitors are required to report to the LSE Estates Division office, Tower One, 4th floor and sign in.

Appendix B: Security Risk Analysis Principles

The starting point for understanding the security environment is to evaluate security related risk. This evaluation should be based on:

- Location and nature of the area
- Building construction and design
- Premises use
- Current access control or other security measures
- Past security record
- Value and desirability of contents

The security risk analysis should be carried out annually or more frequently if there have been changes to the building or the security environment. Once a risk analysis has been prepared it should be evaluated in consultation with the Head of Security. A decision will be made on the level of exposure to security related risk and the appropriate measures to deal with the risk.

Appendix C: Crime Prevention and Security Awareness

All members of staff and visitors to the school must observe the following:

- All suspicious activity must be immediately reported to the Security Team.
- Personal valuables should be locked away or placed out of sight or kept on the person, and personal property should never be left unattended.
- Offices must be locked upon leaving, with ground floor windows closed & locked (where locks are fitted).
- Laptops should be locked out of sight when not in use, particularly overnight. In open areas, laptops should be secured to the desk with a steel enclosure or security cable. Students should make use of the secure storage facilities available. Further enquiries can be made at the Old Building reception.
- Windows and curtains or blinds should be closed at dusk and lights (except security lighting) should be turned off when leaving.
- All incidents of crime on School premises, real or suspected, must be reported to the Security Team.

Appendix D: Personal Safety

The Security Team can provide a great deal of practical advice on how to get the most out of your time at LSE without becoming the victim of crime. For your personal security please keep the following points in mind:

- Avoid walking alone own at night
- Keep your valuables out of sight and carry your bag close to you.
- Be aware of people when using a cash machine and preferably draw out money during the day. Always use the cash machines inside the bank whenever you can. Have a friend accompany you to the cash machine, especially at night.
- Be suspicious of e-mails or phone calls requesting personal information and destroy papers carrying bank or credit card details.
- Do not put valuable items into the general use lockers, particularly wallets, purses and laptops.
- Report any suspicious activity to Security Staff .This helps to prevent and detect crime against the School.
- If you are faced with threatening or abusive behaviour, stay calm, avoid raising your voice and the use of aggressive body language such as finger pointing/wagging. Call for assistance from colleagues and/or Security Staff.
- Secure bicycle storage facilities are available in the NAB and Tower 3. If you use the street bicycle racks, be sure to lock your bicycle even if leaving it for just a minute. Hardened steel D-shaped locks are recommended.
- Secure laptop storage facilities are provided. Enquire at the Old Building reception for more details.
- Take advantage of the free laptop security marking that is offered by the Security Team. This service is offered every Wednesday in the Library lobby.

Appendix E: Lost Property

- All lost and found property will be logged by Security and stored in the lost property office as soon as practical.
- People handing in lost and found property will be issued with a receipt and are encouraged to ask for one.
- 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 property must be signed for.
- All unclaimed articles will be held for a minimum of 90 days. After 90 days unclaimed items will be donated to charity. Any items that cannot be donated will be destroyed. 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.
- The finder of lost property must advise Security if they intend to claim the property if the rightful owner does not. Upon production of the receipt issued when handing in property, the finder may claim the item after 3 months.

Appendix F: Control of Locks and keys

- Any request submitted for new key or locking systems requires authorisation by the Head of Security prior to issue.
- Any request for a digital multi user lock requires the authorisation of the Head of Security. Although these are being phased out and new digital locks will only be installed under exceptional circumstances.
- Any locking solution that is put in place must have an 'override' (i.e. a spare key, master key or code). A copy or details of which must be provided to the Security Team for retention and registration into the security key management system.
- Sub-master keys may be issued to departments for local use and issued to individual staff.
- Departmental administrators should keep a record of all keys and fobs issued locally and ensure that members of staff return keys when they move offices or leave the School's employ.
- It is the responsibility of all individuals who are issued with cards or keys or fobs to ensure their safe keeping at all times and report losses immediately to security staff.
- In every case the loss of a key or its equivalent (a card, fob etc.) must be reported immediately to the Security Team.
- Where additional access control is required Departments/Divisions should discuss their needs with the Head of Security.

Appendix G: Handling Bomb or Suspect Material

- Suspect material, packages or letters should be left where they are and treated with respect.
- Do not open the package or letter, taste or smell any material that may be spilling from the package or letter.
- Evacuate the room or area and secure the area if you can.
- Immediately call the Security Team using the emergency line 666

Appendix H: Security Safety PROCEDURE

The resolution of security related issues involves LSE security staff in endeavours that carry with them substantial risk. The following areas of risk must be considered when undertaking security activity:

- **Physical risk**
The risk of injury or death to security staff, other employees, students, visitors and members of the public.
- **Legal Risk**
This risk that security related activity will precipitate litigation.
- **Reputational Risk**
The risk of damaging the reputation of the LSE is a key consideration. This is particularly acute in relation to the maintenance of free speech and VIP visits.

To minimise the above risks the security the Security Team will carry out a risk assessment prior to the commission of security related activities. In order to carry out a full and relevant risk assessment the Security Team requires information that is as complete as possible. All departments and divisions within the school are responsible for the full disclosure of information as required by the security department for the purposes of security risk assessment.

Under operational circumstances the Head of Security (or his/her nominated representative) will be the sole arbiter of the relevance of information to security risk assessment. Where disclosure is contested it will be reviewed by the legal and compliance team after the fact, to evaluate the case involved and the handling of information to inform the risk assessment process. The legal and compliance team will carry out periodic audits of disclosure to LSE Security to ensure compliance with legislation and guidance standards.

Appendix I: Security Operational Procedures

The LSE Security Team will support the provision of a safe and secure environment in the buildings and communal areas of the LSE main campus by implementing the security operational plans. Security will utilize physical protections systems, procedural methods and protective counter surveillance to achieve the most effective and pre-emptive security model across campus.

Concept of Operations

- The Security Team will provide coverage in 3 8-hour shifts through a 24 hour period.
- Each team is managed by a Team Leader who is supported by a Deputy Team Leader and 9 Security Officers.
- Each team will contain staff trained and equipped to carry out the following functions:
 - Support the effective use of physical protection systems
 - Implement security procedural methods
 - Carry out overt static and roving tasks
 - Carry out covert static and roving tasks
 - Respond to incidents and emergencies
 - Participate in the collection of security data
- The security teams will include the following elements:
 - Static elements in the security control room and at monitoring and reception points.
 - Overt elements throughout the campus to provide a visible deterrence.
 - Covert elements throughout the campus.

Task Organisation and Scheduling

- Early shift will operate between 7am and 3pm
- Late shift will operate between 3pm and 11pm
- Night shift will operate between 11pm and 7am

Data

The Security notebook is a primary source of evidence. All notable facts, anomalies and evidence relating to crimes incidents and other occurrences must be annotated to the notebook.