Security and Risk Management Policy

Background

Middlesex University has always maintained that an open access to its campus is an essential ingredient of academic life. For the Security Team of the University, open access does increase the risk of theft and other types of crimes. The University has recently attempted to reduce the risks associated with having open access by investing heavily in the improvement of security equipment and manpower all of which at ensuring that all members of the university can work and study in a safe and secure environment.

Security is not intended to be a hindrance to academic life but to be an essential ingredient for the smooth operation of schools and departments, especially as stolen or damaged equipment might impinge on the core business of the University. Responsibility for personal property remains with the owner of the property and the University takes no responsibility for such property left on the premises, including motor vehicles and bicycles.

The aim of this policy will seek to formalise a cohesive and integrated approach to security throughout the university.

Policy Statement

The Security Team is part of the Estates and Facilities Management Service (E&FMS) and is responsible for the effective operation and enforcement of the security policy and procedures. Responsibility for security and personal safety rests with all persons who work, study or reside in, or who visit the University and everyone should report all suspicious activity, suspected or actual. All staff, students, visitors or contractors should assist the security department to ensure the success of the policy. Security and personal safety is everyone's responsibility and cannot be left solely as a matter for the security team or Police. The University reserves the right to prosecute and/or take appropriate disciplinary action against any person who acts negligently, dishonestly, or commits a crime against the University. The University will seek to ensure, as far as is reasonably practicable, the security and safety of all staff, students, visitors and contractors, whilst within or situated on the university premises.

Security Management Structure and Responsibilities

. Within this overall responsibility some particular elements are defined as follows:

Senior Management	To ensure that support and resources are available to staff for the implementation of the security and risk management policy.
Director of Estates and Facilities Management Service (this includes the Deputy Director)	Overall development and planning of the security strategy, policies and procedures.
University Security Manager	Development and implementation of security strategy, policies and procedures and the monitoring of their effectiveness and efficiency. Investigations of serious crime or confidential breaches in security; provision of expert and impartial up to date advice; liaison with emergency services, local authorities and outside agencies.
Security Systems Supervisor	Day to day management and implementation of the security policy and procedures; monitoring of the policies and procedures to ensure their continued effectiveness and efficiency. Management and training of security staff, investigation of crime, risk management, analysis and implementation of security solutions, provisions of security equipment, including CCTV, Access control, Intruder alarms, IRIS system, keys, locks, parking systems.
Contract Security Managers / Supervisors	Daily management of the contract security team. Delivery of an effective security service; Management and training of contract security staff, investigation of crime, risk management, analysis and implementation of security solutions, management of security equipment, including CCTV, Access control, Intruder alarms, IRIS system, keys, locks, parking systems.
Contract Security Officers	Security duties as defined in Assignment Instructions and Operational instructions including patrols, locking/unlocking, Event security, reception and access control, dealing with incidents and crime and crime prevention.

Heads of Departments/Schools	Promoting security within their areas. Ensuring staff have access to the Security and Risk Management Policy, ensuring staff and students understand and exercise their security responsibilities, including the showing of I/D cards when requested, have due regard to University property in particular security of IT equipment. Liaising with the security team on matters of security or safety, Undertaking of security risk analysis of their department areas of operation, with support from the security team acting to remove or reduce as far as possible, any security risks including maintaining equipment inventories. Ensuring when a staff member leaves that all keys and I/D has been returned. Informing security of any risk including the purchase of expensive equipment.
Staff Members	This includes all Full/Part, Research and contractors should ensure they are familiar with and follow procedures detailed within the Security and Risk Management policy, paying particular attention to emergency procedures including in the event of evacuations.
Students	To look after university property and to give due consideration to security issues. Security procedures should be followed which have been designed to protect the property of the university. To ensure that instructions passed to them by Security or members of University staff is followed including the showing of I/D cards.

Security Service Performance

E&FMS Security Department manages a Contracted security provider who performs a service of security across the University. The Contractor with instructions from the University and in accordance with UK and EU legislation carry out a wide range of duties from, internal and external patrols, locking and unlocking of buildings, incident management, parking management as well as a list of many other security and safety tasks. The service provided by the Contractor is monitored on a daily basis to ensure that the university is receiving a service that reduces crime across each campus site. The Contract service is reviewed monthly during which time key performance indicators are passed to the company. Any complaints received in regard to the security service performed at the University are fully investigated by the University Security Manager for the University.

Staff training and development

All contract security staff employed to carry out a service to the University are fully trained officers who must pass certain exams and must be cleared by the SIA (Security Industry Authority) before being allowed to work at the University. Each officer must have their SIA licence on show when carrying out duties on University property. The University have also informed the security contractor that all officers must undertake first aid training within three months of working at the University. A further list of courses in regard to security and safety were passed to the contractor as part of their contract to ensure that their staff development continues while at the University. This was seen as vital element to ensure that the university have well trained officers, able to carry out a number of tasks and the ability to deal with any type of incident. Training and development of the contract security team is monitored monthly by the Security Department.

Incident Management and Business Continuity Plans

The university recognises the need to develop and maintain an emergency plan which will allow emergency procedures to be adopted immediately in the event of an incident and to enable the university to return to normal operations as soon as reasonable practicable. The process, formally referred to as the Incident Management and Business Continuity Plan, ensures a consistent proportionate approach to incidents. The plan allows the university to manage;

- emergencies involving physical damage to university assets
- incidents that pose a threat to health and safety of personnel and others
- incidents which effect the operational structure and/or reputation of the university
- incidents that require special measures to restore operations

All Heads of Service and Schools should be fully aware of the plan which is tested on a regular basis. If staff requires further information they should make contact with the University Health and Safety Manager or the University Security Manager.

Raising Awareness of Crime, and Crime Prevention

Proactive crime prevention and security awareness will help to ensure a safe and secure environment for staff, students and the broader community, enabling work and study to continue with the minimum amount of disruption. It is the responsibility of all to counter the threat of crime by reporting such activity to the security team based across the University. The Security Department hold safety events at Fresher's Fayre and other events throughout the academic year. Staff and Students are encouraged to attend these events and obtain safety and security information which can be passed on to colleagues and friends.

Security and Safety Advice

Advice on crime and the precautions to take to safeguard personal and university property can be found on the E&FMS website under the heading of Security and also on the 24/7 website. Contact information for the Security Team has been included on the website if further information is required. The security team would welcome and would provide 1-1, small or large group's presentations on security and safety advice while for on campus or off.

Incident Reporting and Investigations

It is the responsibility of all staff and students of the University to report all activity, suspected or real that appears to be of a criminal nature. Incident reporting is crucial to the identification of patterns of criminal activity. Any report obtained is transferred to the University's Incident Reporting Information System known as (IRIS) all reports submitted are checked by the Security Team. This permits investigations and recommendations to be made to prevent recurrences. Comprehensive reporting of incidents provides an accurate picture of the level of crime throughout the university and ensures that adequate resources are provided to combat the criminal activity. For the Security Team to continue to reduce the amount of crime across the University, fast, efficient and detailed reporting is a key aspect in the fight against crime.

Asset Protection

Staff and students are requested to take reasonable steps to safeguard the equipment belonging to themselves and the University. Taking such steps will help to ensure that the maximum amount of equipment is always available for use at all times. If a department or school are planning to purchase any high valued equipment or are relocating equipment from one area to another a risk evaluation should take place. This information should then be passed to the Security Team so that they can assess the risk and provide measures to reduce the risk of loss. The replacement cost of University property stolen through burglary may be claimed from the University's insurers; however this can only take place where forced entry to the building/room has taken place. University property left in unlocked rooms, unlocked draws or cupboards may not be covered, therefore it is essential that all reasonable steps are taken by staff and students to ensure rooms, windows and desk draws/cupboards are locked when leaving an area unattended, <u>no matter how short the time.</u>

IT Equipment / Computer Misuse

CCSS are responsible for policies and guidance in regard to IT equipment across the university. For advice and guidance on safety of equipment and the use of equipment please contact the CCSS department.

Headed Paper and Confidential Information

University headed paper and any confidential information must be protected to avoid fraudulent use. Confidential information should be locked away when not required. Unwanted information should be disposed of correctly. This can be achieved by purchasing a good shredder that cuts both ways or by using the confidential waste bags supplied by E&FMS. Further information on disposing of confidential material can be obtained by speaking to E&FMS Portfolio Managers or the university security manager

University Security Systems

Requests made to install an alarm, CCTV cameras, locks or access control readers will be subject to a risk evaluation. Departments and schools are requested not to purchase any security equipment without first making contact with the Security Team.

The University recognises that CCTV is a powerful tool in the fight against crime and also as an aid in regard to safety across the University and there are over two hundred cameras in place. The purpose of the University CCTV system is to provide a physical surveillance system that will enhance safety and improve the quality of security; thereby reducing the fear of crime. As far as reasonably practicable the university will create a safe environment by means of physical deterrents without encroaching on the privacy of staff/students and the broader community. If you require further information on the systems please contact the university security manager. If you require

further information on the management of the system or on matters such as Data Protection issues please contact either the university security manager or the university Data Protection Officer

Access Control (Staff and Students Identification Cards)

The University has introduced an access control system for its Hendon campus. Students and staff have a responsibility to ensure that they do not allow a person to enter without using a card. If a staff or student is aware that this is happening they should immediately contact security who will deal with the person. On no account should the staff member or student attempt to deal with the tailgater themselves.

The access control card is also to be used as a staff and student identification card. Once a card is issued it can be used for the library services as well as entry to areas. Planning is underway to increase the use of the card so that a cashless society will eventually be in place across the University. I.e. the card will eventually be used for paying for items from catering outlets, printing and potentially shops off campus.

Visitors and contractors from February 2009 have been able to obtain a card for the day or with permission from the Head of Service/School for a longer period as deemed necessary by the Head. The access control card should be thought of as a key; cardholders should safeguard their card and report the loss of a card immediately once known, so that security can cancel the card. The cards are not transferrable and must not be loaned out to any other person. Disciplinary action may be taken if a card is used in any crime resulting from misuse. Access control cards should be on show at all times, and must be shown when requested. Failure to produce an access control card (Staff or Student Card) may result in the person being asked to leave the premises until verification can be confirmed.

University Vehicle Parks

Middlesex University aims through the Travel Plan to reduce congestion on local roads and ease pressure on campus car parks through the reduction of car use and in particular one-car, one-occupant journeys. As part of the plan, a Car Share Program and pay as you go car park was introduced in September 2008. Revenue raised through car parking charges will be ring fenced for measures outlined in the Travel Plan including better facilities and support for pedestrians and cyclists, promoting and supporting car sharing and the provision of facilities (signage, road marking, lighting and maintenance of car parking as well as security such as an increase of cameras for each campus).

The use of the University Car Share (CS) and Single Occupancy Car Journey (SOCJ) vehicle parks are restricted to card holders only between 0830hrs-1630hrs Monday – Friday. The vehicle parks are controlled by automatic barriers and CCTV. Staff joining the University SOCJ program will be provided with access to car parks via their staff card. The card must only be used by the named staff member and no other person. If a card is found to be used by other person/s the access to car parks will be revoked and the staff member will not be allowed to continue within the parking schemes at the University.

When joining the CS program an access card must be shared between two or more parties. It is the responsibility of the Car share group/pool to ensure that the access card is managed between them, failure to do so could result in the card being cancelled. The issue of an access control card for SOCJ and CS does not guarantee that a parking space will be available for the holder. Parking spaces are allocated on a first come first served basis to holders of the permit/card.

The use of our pay as you go vehicle park at Hendon is restricted to any person requiring to park on University business. The pay as you go car park is managed in the same way as the CS and SOCJ car parks.

Only registered disabled users as defined under the Disabilities Discrimination Act are allowed to park within any disabled bays. In the event that all disabled bays are in use Security will advise alternative areas for parking as near to place of business as possible. Any student or staff member with a short term medical condition, requiring temporary permits should request special dispensation via the University Health advisor or the University Security Manager.

In general, the Vehicle Parking Regulations do not permit the allocation of reserved parking spaces. The University reserves the right however to reserve vehicle parks and vehicle parking spaces on a temporary basis for authorised central University special events and VIP visits. Special arrangements for conferences, meetings, departmental open days etc can be made via the Security Team in accordance with the Procedure on the Use of University Vehicle Parks for Organised Events

The University accepts no responsibility for any accidents or damaged caused to vehicles parking within any university vehicle parks and all owners park at their own risk.

Events

As an educational institution the University arranges and hosts a wide range of events. These include open days, information stands, and educational events, graduation ceremonies, sporting events, shows, parties, student balls and festivals.

The responsibility of ensuring that all events are managed safely rests with the University's Estate and Facilities Management Service (E&FMS). In order to ensure that the level of safety management required is in proportion to the event, it is necessary for the person responsible for the event to us the Event Tool. The Tool helps identify the scope of the event and to assess if enough is being done to reduce risk to as low as reasonably practicable during all the phases of the event. The Tool is based on the Health and Safety Executive's publication: The Event Safety Guide (HSG195), which will be used as the primary source for events. This publication can be obtained from HSE Books www.hse.gov.uk .

It is recognised that some small and low risk events do not need the same level of planning and assessment as medium and higher risk events; therefore there are two types of Events Tool. Generally, it will be common sense which one to use but the E&FMS Portfolio Manager can give specific direction on which one to use.

It is expected that those holding regular and routine events will be able to use generic material for their future events. However care should be taken to ensure the generic material is both comprehensive and specific for each event.

The University has no wish to create additional work, or to put any unnecessary burden on event organisers but it will do what is required to reduce risk to the level required, even if this means cancelling events.

Once the event tool has been passed to E&FMS the Portfolio Manager and University Security Manager will make a decision on what provisions are required. To ensure security staff can be confirmed the event tool will need to be sent to E&FMS Managers at least two weeks in advance of the event. A full quote for the security will be sent to the event organiser. Confirmation and a purchase order number will then be required before any security staff is booked. It is the aim of the E&FMS team to work with you to ensure that all events take place safely and are enjoyed by those who attend.

Definition of an Event

Generally, an event is something that involves a <u>change of use</u> of buildings, premises or the facilities / services. For example a lecture hall is designated as fit for purpose for teaching and for accommodating a prescribed number of students. Therefore the use of the room for teaching (within the set capacities) is not considered an 'event'. However, if it was intended to use the lecture hall to host a social activity this would be a considered a change of use.

Similarly, the Quadrangle at Hendon is an area designed for circulation and reception so using the Quad for an open day and increasing the capacities, inviting members of the public, erecting stands, display equipment, seating, etc would constitute a change of use

Risk Management

Before a security strategy is developed or high valued equipment purchased risks need to be identified. For a security evaluation to be conducted items below need to be addressed;

- Location
- Building construction and design
- Building/room use
- Security equipment installed i.e. alarms, CCTV, access control
- Security measures already employed i.e. extra checks via security
- Past incidents i.e. known high risk area and why
- Value of equipment/ desirability of items

It is recommended that a security review of risks is carried out annually or whenever new equipment is installed, the said area has alterations completed or the area has been involved within an incident i.e. burglary.

When carrying out a risk evaluation please be aware that the risks may vary depending on the time of day and the building usage. For instance, a new open access computer that is in use between 9-6 by students and staff is quite safe so long as students and staff do not leave the room unsecure and unattended. However, during the late hours 6pm -10pm the risks to the room grow when not many people are around therefore the room should change to access control from 6pm, which can then be monitored by Security.

Once a risk evaluation has been carried out it should be checked in consultation with the University Security Manager to decide if the risks are acceptable, what level of protection is required and what priorities should be. An evaluation form can be found at Appendix (1)

For further advice or assistance in completing this evaluation please contact Head of Security: Nick Wise n.wise@mdx.ac.uk

E&FMS Security Department

Appendix (1)   **Self Assessment Form**

Questions	Yes	No	Action Taken/Required	Date
Do you have equipment inventories in place and is this documentation held in a safe place				
Have past action points carried out				
Are there new fire/crime reduction measures in place since last review				
Has there been an increase of crime within your area				
Have you held a meeting with the security manager to obtain incident information or advice on security				
Are your buildings/rooms in good repair				
Is your team aware of security procedures				
Would your team know where to locate security and how to contact them by phone				
Would your team know where to find security and safety information on the intranet				
Are your team aware of emergency instructions including evacuation areas				
Are your team trained in security awareness and to report all suspicious activity				
Have risk assessments been carried out on staff personal safety and procedures				
Do you have a policy of last staff member out to check all doors/windows are secure within your area and that blinds are drawn				
Do you have a clear desk policy to ensure theft of small items or confidential information is not stolen				
Do you ensure your team change their IT passwords at least every 28days				
If you have a safe is the safe bolted to floor/wall, is the safe key locked away, do you change the location of the key often, do you change the access code often, do you ensure only a small number of staff have access to keys or codes, do you ensure money is deposited as often as possible,				
Is lighting effective to deter criminals				
Are your areas covered by CCTV cameras, do you believe them to be effective or do you believe they need relocating to be effective				
Are your areas covered by intruder alarms, do you believe these to be effective, or do they need relocating.				
When staff leave the University, are codes deleted and keys returned, are these details recorded				
Are IT theft prevention measures in place, i.e. locks, chains, PC alarms and cables				

Do you have theft prevention measures for portable equipment such as cameras, laptops, audio-visual equipment such as secure cabinets, safes, secure storerooms (alarmed)				
Are keys held by the department/school recorded, if lost has this been reported to security. When were keys last checked				
If staff deal with cash have they been provided with guidance in regard to handling cash				
If cash is taken from one area to another have you asked advice from security in regard to safe routes, escorts, what to do if scenarios				
Does your department/school use a safe, have you received or asked for advice on safe management/cash handling				
If a safe is used how often is it emptied, are you aware of the safe amount of cash to be stored, how often is the amount checked each day				
Are your staff aware of the incident management plan, how often do you test this system				
Do you ensure that department records are etc are copied and stored in another location from main copies				
Are staff aware of who to contact in the event of suspicious persons or items found, are staff aware not to approach persons acting in a suspicious manner and instead to allow security to deal with the subject				

For further advice or assistance in completing this evaluation please contact the Head of Security Nick Wise. N.wise@mdx.ac.uk