

SECURITY POLICY

1 Introduction

- 1.1 In order for The College to provide a safe and secure environment for students, staff and visitors, a robust Security Policy, along with procedures which will enhance security and safety will enhance current practice without hindering the learning experience. This Security Policy aims to formalise a cohesive and integrated approach to security throughout all college sites.

2 Policy Statement

- 2.1 The College seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors and contractors, whilst within or situated on College premises. The Security & Premises team 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 study, work or reside in, or who visit The College. All students, members of staff, visitors and contractors should assist the security team to ensure the success of the security and personal safety is everyone's responsibility and cannot be left solely as a matter for the security team or police. The College reserves the right to prosecute and/or take appropriate disciplinary action against any person who acts negligently, dishonestly, or commits a crime against The College.

3 Responsibilities

- 3.1 Responsibility for security rests with all students, staff (including contractors and agency staff) and with visitors to The College. In particular, everyone should report all activity, suspected or real, of a criminal nature or any suspicious activity immediately to the security team. Within this overall responsibility some particular elements are defined as follows:
- a. **The Executive:** The College Executive should ensure that support and resources are available to staff 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 should be supported and properly resourced.
 - b. **Estates Manager:** development and implementation of security strategy, policies and procedures with particular reference to health & safety and the monitoring of their effectiveness and efficiency. Investigation of serious crime or confidential breaches in security; provision of expert and impartial up-to-date advice; liaison with police, emergency services and local authorities.
 - c. **Security and Premises Manager:** day-to-day management and implementation of the security policy and procedures; monitoring of these policies and procedures to ensure their continued effectiveness; delivery of an efficient and effective security service to The College; management and training of security staff; investigation of crime; risk management, analysis and implementation of security solutions; provision of security hardware including keys, locks, safes, access control, CCTV, intruder alarm installations etc.

- d. **Security Officers:** security duties as defined in Operational Instructions, including patrolling of all areas, crime prevention, reception & access control.
- e. **Academy Directors:** have a pivotal role in promoting security (alongside safety) within their area. The actual responsibilities will vary according to the location of the school or department and the nature of the activity but a number of specific responsibilities can be identified. (It is recognised that Academy Directors will wish to delegate responsibility for the routine involved in these tasks to a nominated individual in their Academy but the overall responsibility for security matters will remain with the Academy Directors):
 - i. Ensuring their staff have access to and are familiar with the Security Policy, paying particular attention to those issues which are particularly relevant to the activity of their department.
 - ii. Ensuring that all members of staff and students in their department understand and exercise their security responsibilities, including the displaying of College car park permits, and have due regard to College property (see sections below), in particular the security of IT equipment.
 - iii. Liaise with the security team on any security matter and attend security co-ordination meetings if required.
 - iv. Undertaking a security risk analysis (see Section 6) of their department areas and operations, in liaison with the security team and acting to remove or reduce as far as possible, any security risks.
 - v. Maintaining equipment inventories.
 - vi. Controlling access to their departmental areas by taking responsibility for the issue of keys.
 - vii. Ensuring that their departmental staff return to the department, their College car park card and any issued keys on their last day of work.
 - viii. Notifying the security team of any security risk (including the purchase of expensive equipment etc) who will then advise on any additional security or protection and investigate any crime or incident.
- f. **Staff:** (This includes all those with a contract of work, including research staff, visiting lecturers, and anyone employed as tutor, supervisor or lecturer on a temporary basis). All staff must ensure they are familiar with and follow the procedures in The College Security Policy, paying particular attention to those issues which are relevant to their activities. They must also co-operate with requests from the security team, especially with emergency or evacuation instructions and in relation to security procedures.
- g. **Students:** have a general responsibility to look after College facilities properly and to give due consideration to security issues. They must follow security procedures designed to protect College 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 team, especially with emergency or evacuation instructions and in relation to security procedures
- h. **Visitors:** (including conference delegates and event attendees) have a general responsibility to look after The Colleges' facilities whilst on campus and to give due consideration to security issues. In particular they must follow security procedures designed to protect College property and wear their visitors badge at all times. Visitors must follow instructions from the security team or from their host department, particularly in emergency situations.
- i. **Common Areas:** security risks in common or public areas of buildings are the responsibility of The College as a whole but will be the devolved responsibility of the Estates Department. However Academy Directors are asked to draw particular risks or issues to the attention of the security team, so that effective solutions can be proposed in conjunction with all interested parties.

Signed: **Date:** 20 July 2006

Designation: Chair of the Board of Corporation

Policy ref/version number C12/V1

This policy is to be reviewed by the Board of Corporation by July 2008.

APPENDIX ONE (TO THE POLICY) : CRIME PREVENTION

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.

2. Procedure: Crime Prevention and Security Awareness

- All suspicious activity should 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 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.
- Lights (except security lighting) should be turned off when leaving.
- All incidents of crime on College premises, real and suspected, must be reported to the security team.
- Where available the security team will provide Security Officers to patrol internal and external, to aid in the identification of security risks, monitor public safety and act as a deterrent against crime.

3. Incident Reporting

It is the responsibility of all staff and students at The College to report all activity, suspected or real, of a criminal nature. 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 College and thus ensures that adequate resources are provided to combat that crime. Success in The College's fight against crime is greatly enhanced by fast, efficient and detailed reporting.

4. Procedure: Reporting of Security Incidents

- All incidents of a security nature should be reported in the first instance to Security Control on ext 222.
- All available information should be included - time, location, persons involved, items missing.
- An Incident Report Form (available from the security team) should be completed as soon as possible after the event by the person reporting the incident and sent to the Security & Premises Manager.
- The local police should be informed in all cases of reported crimes of assault, indecency, fraud, theft (including car or cycle theft) and burglary. In case of doubt, advice on Police involvement may be sought from the security team. All police involvement on campus is to be notified to the Security & Premises Manager to enable effective College management of any subsequent actions on College premises.
- This reporting procedure should be followed **at all times**.

5. Crime Investigation

All crimes that occur on College premises will be investigated appropriately to prevent re-occurrence and aid crime prevention. The Security & Premises Manager or any member of the security team as appropriate, will be responsible for carrying out internal investigations of security related incidents, producing written reports for circulation where necessary and providing follow up crime prevention advice.

APPENDIX TWO (TO THE POLICY) : ACCESS CONTROL

1. Visitors Pass

- 1.1 Visitors and contractors will be issued with a 'visitors pass' at point of entry and should wear these passes which contain emergency and health & safety information, during their visit to The College and return them on leaving.
- 1.2 Contractors who will be on site for more than a week will generally be issued with a College 'Contractor' card to allow them access to the building they are working in.
- 1.3 All cards must be displayed whilst on College premises.
- 1.4 All staff and students are required to demonstrate their identity and purpose of attendance at The College on request.

2. Weekend and Other Out of Hours Functions/Meetings/Events

- 2.1 The use of College premises at weekends is restricted. Academies or individual staff wishing to teach, run tutorials or organise an event must seek approval from the Executive.
- 2.2 Details of all approved weekend events must be notified to the Security Office at least 7 days in advance so that security cover can be arranged and that checks can be made in case of planned building works etc.
 - Date and timings of function/meeting/event.
 - Location, to include room numbers.
 - Name and department of member of staff hosting/organising the event.
 - Details of any persons attending with special needs (especially for disabled access).
 - Contact telephone number for host.

3. Campus Opening Times

The College buildings are generally open for teaching and related activities from 0830 hrs. The College is generally open until 2100 hrs Monday to Thursday and 1700 hrs on Fridays and vacation periods. Some buildings may be closed after teaching, times of which may vary in each building. Some buildings have automated access control, which allows access for staff & students.

Weekends - Unless opening is specifically arranged for an event (see above), College buildings are closed for general use on Saturdays (afternoons), Sundays and public holidays, as defined in The College Calendar. All campus buildings are closed for a defined period during the Christmas and New Year period.

4. Control of Locks, Keys and Access Control Cards

The Security & Premises Manager controls the issue and use of all locks, keys and access control systems and cards. The College operates a suited key system which allows various levels of access. No other make of lock or key should be installed on College premises without the authority of Security & Premises Manager. Any door, which requires a combination or digital lock fitted (for high usage), must also have a suited key override fitted. Departmental administrators should keep a record of all keys issued locally and ensure that staff return keys when they move offices or leave The College's employment. It is the responsibility of all individuals who are issued keys or cards to ensure their safe keeping at all times and report any loss immediately to security staff.

Where additional access control on The College system is required, departments should discuss their needs with the Security & Premises Manager so that usage analysis and installation can be assessed.

5. Procedure: Request for Locks & Keys

5.1 Staff

- All applications for new cores or keys should be made in writing to the Security & Premises Manager. The request must be authorised by the appropriate manager and forwarded to security at least seven days prior to requirement.
- All issues will be subject to satisfactory fulfilment of criteria to ensure need, use and availability.
- Temporary issue of keys for limited time access (one day or less) may be arranged with the security team at the Site Security Office.

5.2 Contractors

- Keys can, in certain circumstances, be issued to contract staff. Contractors' access to College buildings will be strictly controlled by the security team according to agreed access control procedures. (See Section 2.)

5.3 General

- All losses of keys must be reported immediately to the security team.
- Persons leaving The College or transferring to another site are to return their key direct to their departmental administrator or to security staff. They should not pass it directly to their replacement.
- Replacement keys will only be issued after an investigation of the loss. The cost of replacement may be charged to the Academy, Department or individual concerned.

- All requests for master or sub-master keys are to be made on a Key Request Form direct to the Security & Premises Manager. Any loss of master or sub master keys will be the subject of an inquiry, with all resultant costs for replacement of locks and keys borne by the Academy or Department concerned. Loss of keys may also lead to disciplinary measures should negligence be proved.

APPENDIX THREE (TO THE POLICY) : ASSET PROTECTION: EQUIPMENT DOCUMENTATION

1. New equipment

- 1.1 The safekeeping of all College 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 efforts to ensure that College equipment is protected from the possibility of theft.

2. Procedure: Security of Equipment

- 2.1 For all offices, classroom and staffrooms, all valuable portable IT equipment such as laptops & PDA's, must be locked away out of sight when not in use and especially overnight. A security risk analysis may be conducted by the Security Team (in conjunction with The College's Insurers) at anytime, with any resultant report or recommendations to improve security made to the Academy Directors. Computers should always be password protected and/or switched off when not in use to protect them from unauthorised access to information.

3 Security Hardware

- 3.1 All requests for installations of locks, CCTV, intruder alarm or access control will be subject to a risk analysis. Such equipment is not to be purchased and/or installed (or removed) without prior consultation with the Security & Premises Manager who will advise on approved installers and security response. Where CCTV is installed, the requirements of the Data Protection Act must be followed.

4. Insurance Cover

- 4.1 The replacement cost of College property stolen through burglary may be claimed from The College's insurers but only where forced entry to the premises is proven. Property left in unlocked drawers, or within an insecure/unlocked or un-alarmed area may not be covered by the insurance policy. The insurance policy also has a built in excess of £500.00. Departments are therefore advised to ensure that all valuable items are physically protected as described above.

APPENDIX FOUR (TO THE POLICY) : SECURITY AND INDIVIDUAL RESPONSIBILITIES

1. Security in the Office

- 1.1 It is the responsibility of all staff to be aware of, and familiar with, all procedures that ensure a safe and secure environment for personnel, equipment and documentation in their office areas.

2. Procedure: Office Security

- 2.1 Students and staff should be aware of the 222 emergency telephone line (College hours) for gaining assistance & reporting incidents. Any suspicious behaviour should be reported by telephone to Security on extension 222.

- 2.2 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 and the following locked with keys secured in key cabinets or taken home:

- all internal office doors
- stationery/personnel file cupboards
- desk drawers
- key cabinets

- 2.1 Any departmental keys that have been issued during the day have been returned and any losses reported immediately. Office doors and all windows must be closed and locked as appropriate. Intruder alarms (where installed) must be set. All computers must be switched off or password protected when not in use to prevent unauthorised access to information.

3. Personal Security

- 3.1 Whilst it is the responsibility of the security team to provide a safe and secure environment, it is the responsibility of all students and staff on College premises to take all reasonable measures to ensure their own personal security.

Moving Between College Buildings

- 4.1 Students and staff should make themselves aware of their surroundings and of other people when walking between buildings. Poorly lit or isolated areas should be avoided as should lone working or walking, where possible. Any deficiencies in lighting on College buildings should be reported to the Estates Department as soon as possible.

5. Suspicious Behaviour

- 5.1 If suspicious or criminal activity is noticed, notify or get a colleague to notify the security team on 222. Then if you feel able, question the individual(s) in a customer friendly and positive manner. Security staff will direct security response to the area as a matter of urgency, and if appropriate, ensure the Police are contacted.

- 5.2 Only security staff may attempt to detain but are not to use force in any way. If the individual(s) become argumentative and/or aggressive, security staff are to back-off from the situation and either follow the person at a discreet distance, until off College premises (they are not to be pursued in any way once off College premises) or wait in or around the area until the police arrive to affect an arrest. Security staff should ensure all staff/students in the immediate area are cleared from the area.

Threatening or Abusive Behaviour

- 5.1 Individuals are advised to stay calm and not to use verbal or non-verbal behaviour that may be perceived as being threatening. Assistance is available from the security team by dialling 222. Full procedures are laid out in Appendix 1.

6. Drugs and Illegal Substances

- 6.1 All suspicions of handling or using of controlled or illegal substances should be reported to the security team, in the first instance, so that appropriate investigation can take place. Academies and Departments that hold substances that might constitute a security or safety risk should contact the security team, when appropriate, for advice on best practice.

5. Found Property

- 5.1 Identified found property that is found should be returned to the owner, where it is possible to do so. Where this is not possible, the provisions of paragraph 7.2 should be followed.
- 7.2 Unidentified found property should be handed in to site security staff. 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 finder may then claim the property. (This does not apply to personalised items, financial property, bank cards etc.)

6. Claiming Property

- 8.1 When a person claims an item of lost property, full details will be required. including a full description of the item. For certain items, proof of ownership may be requested. When Security staff are satisfied of the owner's claim, the property will be handed over on signature. Where any doubt to ownership exists, the Security and Premises Manager will be asked to resolve the situation.

7. Property Left in Lecture Theatres or Classrooms

- 9.1 No items of property should be left unattended in teaching rooms. Any property left will be treated as found property and dealt with per paragraph 8 above. Where the value is questionable (leftover hand-outs or teaching material) and/or the condition of the item is poor, the practice has been to treat this as 'unwanted' or 'waste' and it is removed to the skip.

8. Lost Property

- 10.1 Employees or students searching for lost property should contact the site security office. If an item is lost outside College premises the individual should check with the nearest Police Office.

APPENDIX FIVE (TO THE POLICY) : USE OF CLOSED CIRCUIT TELEVISION (CCTV)

1. Reasons For Use

- 1.1 The use of Closed Circuit Television (CCTV) has been recognised as a powerful tool in the fight against crime, both in its prevention and detection. The College uses a CCTV system around the campus covering many of the entrances, main public access areas. It is installed inside and outside buildings, with the objective of assisting to provide a safe and comfortable environment for the benefit of those who work, live and visit The College. This objective will be met through the monitoring of the system so as to:
- Reduce the fear of crime and offer public reassurance.
 - Assist in the prevention of crime and public disorder.
 - Facilitate the apprehension and prosecution of offenders in relation to crime and public disorder.
 - Monitor & deal with any public safety issues.
- 1.2 To comply with the Data Protection Act (1998), (DPA) signs will be placed around The College premises to inform anyone entering the premises that CCTV with recording is in use.

2. Locations

- 2.1 The main College CCTV system consists of both internal and externally located overt cameras with telemetry and digital recording (plus some video recording) based at the main site control rooms. Other buildings have similar but independent systems controlled locally.
- 2.2 It is agreed that some departments e.g. Media and Information Technology Services (MITS) and the Cafeteria may benefit from a local CCTV system for the reasons described above. Future installations in departmental areas, must be authorised by the Estates Department and comply with the DPA.

3. CCTV Operating Procedures

These have been drawn up to ensure that concerns over integrity, confidentiality and ethics are not compromised. It is intended that the information obtained from CCTV or consequent recordings will give public confidence, that the rights of individuals are being fully protected and the requirements of DPA are complied with.

4. Access to the CCTV monitoring and recording systems

It is strictly controlled and is limited to duty security staff or authorised management. The security team have been instructed to not allow access or respond to requests to view CCTV recordings unless with the permission of the Security & Premises Manager and that the provisions of the DPA apply.

5. Police

- 5.1 In general, the police should not require access to (nor be allowed access to) College 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 Security & Premises Manager.
 - At the request of Executive.
- 5.2 Requests by Police to remove CCTV recordings must comply with the DPA and be registered accordingly. For details of this particular procedure contact the Security & Premises Manager.

6. **Recorded Images**

- 6.1 Images will be kept securely at security desks for one calendar month. Any requests to view a recorded image will be dealt with as in 5.3.1
- 6.2 Still photographs from CCTV recordings may be used after an incident by The College's security team to assist in the identification & detection of offenders. They must not be placed in areas viewable by the public or be otherwise distributed. Photographs will be supplied to the police for crime incidents on the basis of a formal request from the responsible Police Officer.

7. **Covert CCTV**

Covert CCTV is employed within The College in specific locations to assist in the detection of crime or apprehension of offenders. Recordings from covert CCTV will be treated in the same confidential manner as above and will be made available for viewing to anyone consequently recorded, in line with the DPA.

APPENDIX SIX (TO THE POLICY) : RISK ANALYSIS

1. Evaluation

1.1 Before hardware is purchased or a security strategy is developed, risks need to be evaluated. This evaluation should include:

- location & nature of the area
- building construction & design
- premises use
- current access control or other security measures
- past security record
- value and desirability of contents

1.2 Risks may vary depending on the time of day, level of building use or if alterations to the building are carried out. A risk analysis therefore needs to be carried out annually or more frequently if there are variations. Once a risk analysis is prepared it should be evaluated in consultation with the Security & Premises Manager, to decide if the risks are acceptable, what level of protection is required and what the priorities should be.

2. Ten Principles for Risk Analysis

When carrying out a risk analysis, remember the three R's — 'Reasonable', 'Realistic' and 'Risk Commensurate'. Where perhaps funding is limited and risks are considered low, often a simple solution can be just as effective as a more complex one. e.g. do you need an intruder alarm or a window lock? (which is a cheap and effective investment to prevent burglary.) Consider the following when carrying out a risk analysis:

3. Target Removal

Permanent or temporary removal of the target (valuable item). Quite simply this means ensuring the target is not visible from outside or is removed from public view.

4. Target Hardening

Make the target resistant to attack. Expensive IT equipment should be fitted within a steel enclosure or in a purpose made IT desk with security bolt. Where possible doors should be solid, within a strong frame and filled with adequate locks.

5. Remove the Means to Commit the Crime

Ensure that anything an offender may find useful to assist them, such as keys, tools, ladders etc are locked away and not left easily accessible. Scaffolding should be enclosed at ground level to prevent climbing and an intruder alarm fitted at the first lift.

6. Reduce the Payoff and Loss

Property marking expensive items with The College postcode and the department name, reduces the potential for resale and increases the chance of the property being returned if found. Insurance cover is available but limited and the Policy excess may not cover the loss.

7. Access Control

Where possible, restrict access to a room, area, floor or building using access control. This can be part of The College's electronic card access system, video/entry phone system, a digital combination lock, or traditional key lock.

8. **Visibility and Surveillance**

Three methods of surveillance should be considered:

- Natural — the area is visible to other occupants or passers by.
- Formal — using technology &/or people to monitor the area & deter offenders and having a procedure to deal with suspicious persons.
- Informal — encouraging employees to be vigilant.

9. **Environmental Design**

Pulling in a range of security measures at the design or planning stage of a building or refurbishment, to reduce the risk of crime.

10. **Rule Setting**

Local procedures as well as College Policy should be used. e.g. efficient evening locking up procedures for offices and IT rooms; local key issue and controls; a 'communication tree' for passing on important security information; exit procedure for staff who leave (to hand in ID card & keys and change access codes).

11. **Increase the Chance of Being Caught**

Any measure that slows down an offender or increases the chance of them being caught can be considered. The longer it takes to commit an offence the more vulnerable the offender feels. Some of the other principles cover this, such as target hardening, but also consider publicising security detection (CCTV warning signs) and any successes when criminals are caught.

APPENDIX SEVEN (TO THE POLICY) : SECURITY RISK ANALYSIS – SELF ASSESSMENT FORM

Security Risk Analysis

A security risk analysis should be carried out annually or whenever circumstances change which may affect security measures. This form is provided as an aide to self-assessment and does not necessarily cover every security circumstance or possibility.

	QUESTION	YES	NO	N/A	ACTION/COMMENTS
A	General:				
1	Are your equipment inventories up to date? (These should list your valuable equipment with serial numbers, values etc and can be produced to identify property subsequent to theft, arson or vandalism)				
2	Have all the action points been carried out from your last security analysis?				
3	Have any crime or fire reduction measures been added since your last analysis?				
4	Have there been any incidents of crime or suspicious activity in your area?				
5	If 'yes' to previous question, have incident forms been completed & returned to Security Team?				
6	Has damage from any previous incidents been made good or improved to discourage re-offence?				
7	Has any guidance been sought on security measures from the Security Team?				
B	Staff:				
1	Are new staff briefed on The College and any local Security Policy and Procedures?				
2	Are all staff trained in security awareness & to report suspicious activity, maintenance issues etc?				
3	Has a risk assessment been carried out on staff personal safety & any safety procedures published?				
4	Do staff know College emergency procedures?				
C	Building Security:				
1	Are the premises in good repair?				
2	Are all doors locked when areas are vacated/not in use?				
3	Are windows closed when rooms/areas are not in use?				
5	Is good housekeeping in force to remove easy methods of access for offenders?				
6	Is lighting effective (to deter intruders)?				
7	Have intruder alarms been installed in high value or vulnerable areas?				
8	Are intruder alarms working correctly and hardware maintained?				
9	Is the alarm system set & unset each time the area is not in use?				
10	Are intruder alarm codes deleted from the system whenever someone leaves?				
11	Are IT theft prevention measures in place (High value equipment out of sight, PC enclosures in use etc)?				
12	Are there secure storerooms or containers for securing attractive portable items such as laptops, camera, audio-visual equipment etc?				

D	Keys:				
1	Is there a proper system to control the issue of keys?				
2	Are lost or stolen keys reported to the Security Team?				
3	Are locks changed when a key is lost?				
4	Is there an established procedure for locking up?				
E	Cash:				
1	Does the department handle cash?				
2	If 'yes', are staff trained in cash handling procedures (see College Financial regs)?				
3	Is cash counted and stored out of sight?				
4	Is money stored in a safe and keys locked away?				
5	Are cash holdings kept to a minimum?				
6	Is cash handling audited regularly?				
F	Visitors:				
1	Is the building reception notified of expected visitors & badges arranged?				
2	Are visitors collected from reception and escorted during their visit?				
3	Are unexpected or previously unknown visitors asked for identification?				
4	Are visitors/members of the public prevented from entering unauthorised areas?				
5	Do staff challenge strangers in unauthorised areas?				
G	Security outside office hours:				
1	Do staff check that students & visitors have vacated staff areas at the end of the working day before locking up?				
H	Contingency Planning:				
1	Do you notify the Security & Premises Manager when there are changes to out of hours contacts? (for The College Emergency Management Plan)				
2	Does the department have a local emergency or contingency plan to reduce or minimise disruption on activities after a serious incident?				
3	Are duplicate records & back-up copies of computer files maintained regularly and kept in a separate location?				
4	Is there a department 'communications tree' for emergency contact? (Including out of hours)				