

Author: Tracy Phipps, Head of Security Services

Date: 07/09



Date	Version	Author	Comments
07/09	D01	Tracy Phipps	Original Policy - Draft
02/10	D02	Tracy Phipps	Updated and Ratified by Steering Committee

University of Warwick Security Policy

Contents

Introduction	2
Background	3
Policy Statement	4
Responsibility	5
Appendix A: Extract – financial regulations and procedures	8
Appendix B: Extract: CCTV Code of Practice	9
Appendix C: Management of Contractors	12

Author: Tracy Phipps, Head of Security Services

Date: 07/09

Introduction

The University of Warwick is arguably the most successful of UK universities founded within the past half-century, and has earned an outstanding reputation both for research and teaching. The University's main campus is located on a 400-acre site spanning the south west boundary of Coventry and the county of Warwick. Founded in 1965 Warwick has been a unique and uniquely successful British university combining a "can-do" entrepreneurial spirit with a commitment to absolute academic excellence.

Open access to a university site is rightly seen as an essential ingredient of academic life. It is also important that the University is seen to be a good neighbour adding value to the community. In that respect the campus offers excellent sporting facilities, which are open to the local community, including a swimming pool, a newly refurbished gym, a climbing wall, an all weather running track and acres of football and rugby pitches. An indoor tennis centre has recently been opened. The renowned Warwick Arts Centre is one of the largest outside London with the Mead Gallery showing visiting collections of contemporary art, a concert hall, two theatres and a cinema.

In terms of transport there is a regular bus service to and around the campus from the city and surrounding areas. On any one day there may be in excess of 500 cycles present on Campus and on average over 5000 vehicles come onto the campus during each working day. The University of Warwick is easily accessible from London, Birmingham, and Leicester and is close to many of the countries major arterial routes, including the M40, M5, M6 and M1.

Open access to the University does, therefore, carry inherent security risks and if the general invitation to the public onto the campus is not to be abused regularly, some security measures are not only inevitable but highly desirable to maintain the University's reputation as a safe and secure place. This Security Policy therefore seeks to formalise an overall integrated approach to security on the main campus and its related sites.

Author: Tracy Phipps, Head of Security Services

Date: 07/09

Background

The University of Warwick has a turnover approaching £400 million and its fixed assets include 110 buildings over three sites. The University is committed to future investment in its campus infrastructure and environment, with a projected 40% increase in size over the next few years. The assets of the University are protected by a 24hr in-house Security team as well as over 2000 intruder alarms/detection devices, over 500 Access control readers and over 300 CCTV cameras.

Warwick employs over 5,000 members of staff, of whom 2,400 are academic and research staff spread across academic departments and research centres; It has a total student population of 17,000 (full-time equivalent) of whom approximately 11,000 are undergraduates and 7,000 are postgraduates. Many of Warwick's staff originate or were educated overseas and almost a third of the total student population comes from over 120 countries outside of the UK. Ensuring the safety and security of such a large and diverse population is the responsibility primarily of the Security team, but this has to be supplemented at all times by security awareness amongst the population itself.

Policy Statement

The University of Warwick is committed to ensuring as far as possible a safe, secure and friendly environment for students, staff and visitors, free from injury, personal threat, damage and theft.

Responsibility for security rests with all persons who work, reside or study within the University community.

Responsibility

Responsibility for security rests with all staff and students of the University and visitors to the campus. Within this overall responsibility some particular elements must be defined

The University Council

The University Council is the executive governing body of the University with particular managerial responsibilities for finance and the University estate, and also a more general remit to oversee the conduct of University business in concert with the Senate. The Council is ultimately responsible for approving this Policy and ensuring that those relevant bodies and individuals responsible for its implementation are appropriately identified. The Audit Committee of the Council monitors the framework of internal controls operating within the University, including those relating to Security.

Senior Management

Senior management of the University must ensure that support and resources are available to staff for the implementation of the Security Policy. Some key tasks which must be undertaken will be time consuming: this is particularly so with Security Risk Assessments. Necessary measures to improve security in essential areas must receive priority consideration wherever possible. Where necessary, the concept of specific training to achieve acceptable standards of operating must be supported and resourced. The Registrar has overall responsibility for the provisions of administrative services to the University. The responsibility for security is delegated to the Deputy Registrar and discharged through the Head of Security Services.

Head of Security Services

The responsibilities of this post include the provision of expert up-to-date advice, liaison with police and emergency services and liaison with contractors for security equipment. The Head of Security Services should also assist Heads of Department to produce an analysis of security risks and to achieve effective but workable solutions to identified problems. The role should, in conjunction with Internal Audit, provide an inspectorate function to ascertain that measures are being implemented correctly.

The Head of Security Services also has responsibility (in consultation with the Registrar and Deputy Registrar) for coordinating the Security requirements of official and VIP visits, including those involving members of the Royal household.

Heads of Department

The pivotal role in promoting enhanced security lies with Heads of Departments. Security is not intended to be a hindrance to academic activity but to assist with the smooth operation of a department, particularly when financial constraints mean that stolen equipment might not be replaced immediately or even at all. The actual responsibilities will vary according to the location of the department and the nature of the activity but a number of specific responsibilities can be identified for Heads of Department:

- Ensuring familiarity with all of the contents of the Security Policy, paying particular attention to those issues which are relevant to the activity of their department.
- Undertaking a security risk analysis of the department, in liaison with the Head of Security, and acting to remove or reduce as far as possible any security risks.

Author: Tracy Phipps, Head of Security Services

Date: 07/09

- Maintaining an inventory of equipment as laid down under the University's *Financial Regulations and Procedures* (see Appendix a) for expensive items, or those which otherwise require particular protection. A record should be kept of the product name, the manufacturer's name, the model number and serial number.
- Authorising access to the department by the issuing of keys or setting of access control zones and confirming in writing to the Security Reception which staff may have access to areas which are locked out of office hours.
- Ensuring that all members of staff and students of the department understand and exercise their security responsibilities and exercise a duty of care with regard to University property

IN THE CASE OF ANY SINGLE ITEM OF PROPERTY PURCHASED EXCEEDING £100,000 IN VALUE AS AN ASSET FOR THE UNIVERSITY, THE PROPOSED PURCHASE MUST BE NOTIFIED TO THE HEAD OF SECURITY WHO WILL HELP TO ADVISE ON SECURITY AND PROTECTION.

It is recognised that Heads of Department will wish to delegate responsibility for the routine operational matters involved in these tasks to a nominated individual in their Departments **but the overall responsibility for security matters will remain with the Head of Department.**

Employees

Employees of the University have responsibility for:

- Ensuring that if they use University property that its security has been properly considered and that effective measures are taken to prevent loss in appropriate cases. As a general rule, any collection of ready cash, instantly convertible commodity and all property worth in excess of £300 which represents an attractive target for thieves must be protected by some means.
- Ensuring that the area they work in is properly secure at the end of the working day with all windows being closed and doors securely closed and locked. Where such devices are fitted employees are responsible for the setting of provided alarm or protective systems. Where offices or work places are temporarily left unoccupied, employees must ensure windows are secured and doors properly locked.

Responsibility for personal property always remains with the owner of the property. The University takes no responsibility for such property left on the premises and this includes motor vehicles and cycles although Security staff will do their best to provide a security presence across the campus at all times.

Security staff including porters

Security staff, including Building Porters, are responsible for the co-ordination and monitoring of security procedures and protection systems. They will arrange for lock-up and opening procedures to be carried out as agreed with Departments. Out of term time and during main holiday periods, Security staff will be responsible for controlling access to secured parts of campus and will not admit unauthorised persons. If a person* who does not hold a relevant key or the appropriate access on their University card requires access to a building or department during vacations or when the University is closed, then this must be certified in writing by the Head of Department to Security Reception. A member of Security staff will then provide access for authorised persons on request.

** It is accepted that postgraduate students may often require access to departments: the relevant Head of Department should make appropriate arrangements.*

Students

All students who make use of University property and facilities have a general responsibility to look after these facilities properly and to give due consideration to security issues. They must follow security procedures designed to protect University property, in particular regulations governing access to science and computer labs or areas with other sensitive equipment.

As indicated for employees, responsibility for personal property always remains with the owner of the property. The University takes no responsibility for such property left on the premises and this includes motor vehicles and cycles although the Security staff will do their best to provide a security presence across the campus at all times. Students who are resident on campus are advised to ensure that they secure all windows and lock their study bedroom doors when they leave their residences.

Advice on information on security issues for students is provided by the Security department and also the Student's Union Welfare Officer.

Visitors to the Campus

All visitors who make use of University property and facilities have a general responsibility to look after these facilities properly and to give due consideration to security issues. In particular they must follow security procedures designed to protect University property.

Responsibility for personal property always remains with the owner of the property. The University takes no responsibility for such property left on the premises and this includes motor vehicles and cycles although the Security staff will do their best to provide a security presence across the campus at all times.

Common or shared areas

Where areas of buildings are common or shared with other Departments the security risks in those areas are shared by all the Departments that use that area. Heads of Departments in these areas are asked to draw particular risks or issues to the attention of the Head of Security so that effective solutions can be proposed in conjunction with all interested parties.

Appendix A

Extract – financial regulations and procedures

Loans of University property

No University property should be removed from the University premises without the prior permission of the Head of Department. Any assets owned or leased by the University must not be subject to personal use without prior approval from the Finance Director. This includes free issue software provided under licence. This permission would only be given in exceptional circumstances. The purchase, lease or rent of assets must comply with Financial Regulation H and Financial Procedures [18](#), [19](#) and [20](#). Reference must be made to HEFCE requirements where exchequer-funded assets or exchequer funds are involved.

Inventories

In the accounts of the University, equipment costing less than £25,000 including (£1,000 for subsidiaries) per individual item or group of related items, and vehicles costing less than £5,000 are written off in the year they are purchased. As these are written off they are not recorded in the University's Central Fixed Asset Register which is maintained centrally within the SAP finance system. As such, there is a need for Departments/Centres/Activities to keep a record of all of these assets and to make sure this is kept up to date.

Heads of Departments/Centres/Activities are responsible for establishing and maintaining adequate arrangements for the custody of stocks and stores within their Department/Centre/Activity.

Those Heads of Departments/Centres/Activities whose stocks require valuation on the balance sheet must ensure that regular inspections and stock checks are carried out.

Stocks and stores of a hazardous nature must be subject to the appropriate security checks and Health and Safety procedures.

Disposal of Assets

In order for the University to ensure that its central fixed asset register is kept up to date, Departments/Centres/Activities must communicate to the central finance office (Finance Manager (GAT) on behalf of the Head of Group Accounting Team) where they become aware of changes in capitalised assets (for example where any of these assets are disposed of or where their value has fallen due to damage or changes in market conditions).

Disposal of equipment and furniture must be in accordance with Financial Procedures FP20 section 20.3.2(d). This includes disposal of equipment originally purchased with the aid of a grant from an outside body.

The Finance Director should be informed of any item which has previously required special insurance cover, which is sold, or otherwise disposed of, as the insurance arrangements may need to be amended or unexpired premiums recovered.

University Vehicles

The Director of Estates is responsible for all University vehicles. This responsibility includes acquisition and disposal, taxation, legal compliance and maintenance arrangements. Insurance is the responsibility of the Purchasing and Insurance Office.

Author: Tracy Phipps, Head of Security Services

Date: 07/09

University vehicles may only be used on University business. The prior consent of the Department/Centre/Activity Head to meeting the cost of a journey must be obtained. The use of these vehicles by staff or others in a private capacity is not permitted.

Losses of University property

Any losses must be notified immediately to the Head of Security. Finance Director should also be advised so that an insurance claim can be made where appropriate.

Appendix B

CCTV Code of Practice

Each department will sign an agreed operating procedure which is specific to their individual operation. This will govern the use of their system in compliance with the Code of Practice and procedure manual. This form of agreement can also cover other bodies with valid interest / cause for access to data, such as the West Midlands Police and the Warwickshire Constabulary.

- Material covered by 'The Agreement' must be kept in a secure cabinet, in a place that only authorised staff have access to.
- The material must only be available to authorised members of staff.
- The material must not be copied in any form.
- The material must not be removed from its designated secure place.
- The material must not be published without the written permission of the Data Controller.
- The material must not be distributed.
- The material must be returned to Security on request.
- The contents of any written material must not be divulged to unauthorised staff.
- Any staff given access to the material referred to in this document, must be informed regarding these restrictions.

1. Reviewing of information.

Reviewing of information, voice recording or video imagery will be carried in compliance with the relevant legislation and procedures, by those who have a signed agreement and method of managing the material in their possession.

2. Distribution of information.

Any information, recordings or still images will only be distributed / shared in compliance with the relevant legislation and procedures, to those who have a signed agreement and method of managing the material in their possession. Only authorised person(s) can be given custody of data, recordings or still images.

They must not only be issued the agreement, but be instructed to ensure their understanding of these documents. They must also complete a form stating who will have access to the information.

3. Copying of material.

Copies of material will only be made for a valid, specific reason, the original, copy and still image(s) being managed / distributed in the prescribed manner. Copying will only be carried out by authorised security staff, to ensure that no unauthorised copies are made. All copies will be labelled with cross reference numbers to the original, each copy having its own reference number. The distributed material must be returned to the authorised security officer for disposal on request.

4. Security of Equipment, Images and Recorded Material.

Reasonable steps must be taken to ensure that live and recorded images are not accessible to unauthorised persons. This procedure addresses the security and access to recording systems and the material itself.

- All recording equipment must be secured in a locked cabinet, preferably in a room that is locked when not in use. If the system is PC based, or has remote keyboard access, these functions must be password protected.
- All images and CD's must be stored in secure containers/cabinets.
- Removal of CD's or recorded material from the system must be recorded
- Only authorised persons to have access to the recorded material and direct view of monitors.
- It is a criminal offence to give access to or disclose recorded data/images to person(s)/organisations other than allowed within the procedures and by the process as directed by this policy/operational procedure. ('The Data Protection Act 1998')

5. Installation and Planning.

Prior to the installation of new systems, the aims and intentions for that systems use are to be analysed and recorded. The type of system used must be adequate and efficient for the intended use. Local physical conditions will have a bearing on the type of system/equipment installed.

The planning and installation of equipment will be overseen by the data controller. On completion of the installation, the suitability and efficiency of the system will be inspected by the data controller, the result being recorded.

The following points are to be considered when planning an installation;

- Intended use. Operational Requirements of every Camera must be recorded in accordance with BSEN50132
- Intended duration of use.
- Physical conditions at location.
- Operation of the system.
- Signage
- Possible areas overlooked. (privacy)

6. Privacy and Confidentiality

The privacy of students, staff and visitors to The University of Warwick is of paramount importance. Where ever possible, surveillance equipment should be sited to prevent undue or unnecessary intrusions to the privacy of the above, and to members of the public who live adjacent to the university or simply pass through it.

If equipment can be installed so that it is physically impossible to invade anyone's privacy, this must be done. If, however, the need for the equipment and its operating requirements preclude the above, the following must be ensured:

a. Surveillance / Monitoring

- Staff who operate CCTV systems must be made aware of the implications of instances of invasion of privacy.
- **It Is Regarded As Gross Misconduct To Unnecessarily Invade a Persons Privacy.**
- CCTV systems must not be used to observe private residences adjacent to The University's property.
- To unnecessarily monitor or zoom into a person, vehicle, office or campus residence is an invasion of privacy.
- For training purposes, it is reasonable to practice surveillance techniques with the CCTV system, but these occasions must be noted in the Console Log.

b. Recording

- It is an invasion of privacy to unnecessarily record images
- Images that are retained pending enquiries, must be destroyed / erased once they are found to be of no significance
- All material retained for future review must be recorded in accordance with the procedure set out in this document
- All recordings of incidents, suspicious persons / vehicles must be entered in the Console Log, with details outlining the reason for that recording, also the retention of the tape or its immediate erasing.

Appendix C

Management of Contractors

Work Covered

- Visiting the site to survey work to be carried out and carrying out the survey.
- Carrying out installations, maintenance and services in Plant Rooms, departments, teaching areas, offices, basements, cellars, trunking and roof areas.
- Carrying out new building, extending existing buildings, remodelling and refurbishment programmes.
- Maintaining plant, services or equipment whether as part of a Service Agreement or not.

Site Arrival - Staff and Agents Must:

- Report to the nominated individual on the official Contract/Order, Workshops, Porter or Security Reception unless the site is self-contained and under Contractor control.
- Sign the Departmental Visit Book (where there is one) and sign for any keys necessary to complete work.
- State vehicle details and name of firm.
- State own name and working location.
- State time of signing in.

Completion of Work or End of Working Day

- Report to nominated officer, Porter or Security Reception unless working in a self-contained area in which case these provisions apply at the end of the contract.
- Sign out stating time and return all keys.
- Leave site. The University accepts no responsibility whatever for Contractors tools, plant or equipment whilst on site and anything left, including personal property, is entirely at Contractor or individual risk. In appropriate cases, perhaps because of the nature of the site, the University reserves the right to insist on site security, 24 hours a day, 7 days a week, at the Contractors expense.
- **ANY CONTRACTOR WHOSE STAFF ARE RESPONSIBLE FOR TAKING KEYS OFF SITE IS LIABLE TO BE CHARGED FOR REPLACEMENT LOCK SUITES AND KEYS WHERE THE UNIVERSITY DEEM IT NECESSARY TO REPLACE FOR SECURITY REASONS.**

Duties and Responsibilities

Contractors must make themselves aware of hazards in those areas where they will be working. The University Safety Policy is available through the Health and Safety Office as is the Contractors' code of safe working practice. Contractors, their staff and sub-contractors must not routinely access areas of the University unnecessary to the completion of the contract. Any blockage to any University road must be notified to Security 5 working days before it becomes necessary. In the event of an emergency road blockage, Security must be notified immediately. All signage must be provided by the Contractor and is expected to conform fully with all relevant Health and Safety regulations. Contractor vehicles must be registered with Security or the relevant project manager and parked in designated areas. The University parking control regulations apply to Contractors and prohibit other parking except by the display of an appropriate permit or ticket. In particular, disabled parking bays must be kept clear. As must areas adjacent to Emergency Exits from buildings.

Exchange of Information on Hazards

Where Contractors work is expected to or does create special hazards, for instance heat application or use of hazardous chemicals or substances, the Area Safety Officer and the staff in the Department or area must be notified before work commences so that relevant precautions can be taken.

Work Outside Normal Hours

"Normal hours" are defined as Monday to Friday 9 a.m. to 5 p.m. excluding public holidays. If work needs to be done or continued outside those hours, prior agreement must be sought from the nominated person in the University who will then be responsible for notifying Security. In an emergency, Security must be informed and the area secured at the conclusion of the emergency work.

Internal Arrangements

Where Contractors have exclusive occupation of an area for their work, then it is incumbent on the Department staff concerned to ensure that there are no confidential materials left within that area unless it is securely locked away and the key remains out of Contractors possession. Where a Contractor requires access to a particular room, then the occupant of that room should first be consulted and arrangements made to accompany the Contractor. Someone from the Department must remain with the Contractor whilst he is in the room concerned where it is safe to do so. In the total absence of the occupant of the room, then the Head of Department concerned will decide on access. Mostly, it must be remembered, Contractors are here to do work for the University and it should be the aim of University staff to facilitate that process but not at the expense of endangering security in a particular room or area where this is a consideration.

In the case of Estates staff, they will usually be responding to a reported fault in which case they should be granted unaccompanied access wherever they require unless it is felt specifically necessary to accompany. Estates staff are also likely to respond to emergency calls and to visit various places for routine purposes. They should be known to most members of staff anyway but in doubtful cases will need to produce their University cards for inspection.

In the absence of any responsible person within the Department, and where access to an area is required, Security may be able to take on the task of allowing access and supervising where necessary, if this does not interfere with the operational running of the Security department.