Fairfield School of Business

School Security Policy

Version:	**2.2 (November 2022)**
Category:	Safety, Security and Environment
Owner(s):	Deans; Head of Estates and Resources
Approved by:	The Board of Governors
Access:	**Public** – Anyone can view this document
Scope:	This policy applies to all staff (including contractors and volunteers), students and visitors at Fairfield School of Business (FSB)

Contents:

If you see or suspect something which may be a security breach, report it to your Campus Health and Safety Nominee or the Front of House Team immediately.

If there is a medical emergency or grave danger to life, the correct procedure is to call 999 immediately and request the emergency services, then inform the Front of House Team.

1. Policy Statement

1.1. The School will endeavour to ensure, as far as is reasonably practical, the personal safety and security of all students, staff and bona fide visitors on its premises.

1.2. The Operations Department is responsible for the effective operation and enforcement of the Security Policy.

1.3. Responsibility for security and personal safety rests with all persons who study, work or reside in, or who visit the School premises. All students, staff, visitors and contractors should assist the Security Team and related personnel to ensure the success of the Policy.

2. Responsibilities

2.1. Responsibility for security rests with all students, staff and visitors to the School. Everyone should report all activity, suspected or real, of a criminal nature or any suspicious activity immediately to the security staff. Within this overall responsibility some elements are defined as follows:

I. **The Senior Management** of the School 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.

II. **The Operations Manager** is responsible for overall development and planning of security strategy, policies and procedures and overseeing the operation of the Security Section, - 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 service to the School; management and training of staff; investigation of crime; advice on implementation of security solutions, security hardware, CCTV, intruder alarm installations etc.

III. **Security Officers** are responsible for conducting their duties as defined in Operational Instructions, including patrolling of external areas to deter trespass, daily unlocking/locking procedures and access control for out of core hour events, caretaker duties.

IV. **All staff** must ensure they are familiar with and follow the procedures in the School 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 in emergency or evacuation situations and in relation to security

procedures. Staff are required at all times when on School property to carry their School cards.

V. **All students** have a general responsibility to look after School facilities properly and to give due consideration to security issues. They must follow security procedures designed to protect School 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 in emergency or evacuation situations and in relation to security procedures. Students are required to carry their School cards with them at all times and when on School property.

VI. **Visitors** have a general responsibility to look after the School facilities whilst on campus and to give due consideration to security issues. In particular they must follow security procedures designed to protect School property and where issued, wear their visitors' badge at all times. Visitors must follow instructions from the Security Team or from their host department, particularly in emergency situations.

3. Crime Prevention

3.1. 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.

Procedure: Crime Prevention and Security Awareness

In general:

- All suspicious activity should be immediately reported as set out in 1.2 below.
- Personal valuables should be locked away or placed out of sight or kept on the person, and personal property should never be left unattended.
- Laptops and other portable IT/AV equipment should be locked out of sight when not in use, particularly overnight, in open areas.
- All incidents of crime on School premises, real and suspected, must be reported to the Security Team.
- Where available Security Officers will make patrols of the premises, to aid in the identification of security risks, monitor public safety and act as a deterrent against crime.

3.2. Incident Reporting

It is the responsibility of all staff and students 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 School and thus ensures that adequate resources are provided to combat that crime. Success in the School's fight against crime is greatly enhanced by fast, efficient and detailed reporting.

Procedure: Reporting of Security Incidents

- All incidents of a security nature should be reported in the first instance to the Security Team.
- All available information should be included - time, location, persons involved, items missing etc.
- The victim in all reported cases of all crimes, but in particular assault, indecency, fraud, theft (including car or cycle theft) and burglary are advised to inform the local police. In case of doubt, advice on Police involvement may be sought from the Head of Operations.
- Criminal Offences committed by Students should be reported to the Police by the Head of Operations
- All Police involvement is to be notified to the Head of Operations to enable effective management of any subsequent actions on School premises.

3.3. Crime Investigation

All crimes that occur on School premises will be investigated appropriately to prevent re-occurrence and aid crime prevention. The Head of Operations or other members of the Security Team as delegated will carry out internal investigations of security related incidents, producing written reports for circulation where necessary and providing follow up crime prevention advice.

4. Access Control

4.1. School ID Cards

All staff and students are issued with an FSB card which is used as an identity (ID) card, a student registration card, and a Library membership card. Students are required to carry their ID card with them at all times and to show their card to officers or employees on request. Staff are required under the terms of their employment contracts to carry their card at all times whilst on School premises. Loss of one of these cards should be reported, as soon as possible to the IT helpdesk.

Access Control Systems operate in some areas. Card controlled barriers/doors are an effective method of preventing unauthorised access and the security strategy will move towards expansion of access control systems throughout the School. Access cards should be regarded for security purposes the same as a key. Cardholders must safeguard their card and report any loss to the IT helpdesk as soon as possible, so the card access can be cancelled.

Visitors and ad-hoc Contractors will be issued with a 'visitor pass' at point of entry and should wear these passes which contain emergency and health & safety information, throughout their visit to the School. The member of staff responsible for the visitor/contractor should ensure that they collect the visitor's pass when signing out upon leaving the campus.

All staff and students are required to show their School card to security staff on request. Failure to do so may result in an immediate request to leave School premises if a person's identity cannot be confirmed.

School Management Team may liaise with the Security Team to arrange for random checks of School cards and Student cards.

4.2. Procedure: Out of Hours Access

Staff who require access to work in their office outside normal opening hours, need written permission from the Head of Operations.

4.3. Control of Locks, Keys and Access Control Cards

The Operations Department controls the issue and use of all locks, keys and most access control cards. No other make of lock or key should be installed on School premises without the authority of the Head of Operations. Operator keys or sub master keys may be issued to departments for local use and issue to individual staff.

Departmental administrators should keep a record of all keys issued locally and ensure that staff return keys when they move offices or leave the School'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 Head of Operations.

Procedure: Request for Locks & Keys

All keys belong to FSB and are not exclusive. Security requires access to all areas especially in emergency situations. Any request made by Security for keys (or access to keys) codes; swipe cards; any others means of access must be granted in order that emergencies (especially out of Core Hours) can be dealt with immediately. In exceptional circumstances certain restrictions may apply to sensitive areas but agreement should be achieved between interested parties regarding access in any emergency.

Staff

- All applications for new keys should be made via a request to the Head of Operations.
- All issues of keys will be subject to satisfactory fulfilment of criteria to ensure need, use and availability.

Contractors

- Contractor access to School buildings will be strictly controlled by the Security Team according to agreed access control procedures.

General

- All losses of keys must be reported immediately to the Head of Operations.
- Persons leaving the School are to return their keys direct to the Head of Operations or HR Department as appropriate. They should not pass keys directly to their replacement.
- Replacement keys will only be issued after an investigation of the loss. The cost of replacement will be charged to the School, department or individual concerned.
- 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 School or Department concerned. If loss of master or sub master keys is suspected to have arisen through negligent action by a member of staff, then an investigation under the appropriate Disciplinary Procedure should be undertaken. Further disciplinary action may be taken if appropriate, following the completion of the investigation.

5. Asset Protection: Equipment/ Documentation

5.1. Security of Equipment

The safekeeping of all property will help to ensure that the maximum amount of equipment is available for use at all times. Students and staff are to make all possible effort to ensure that all equipment is protected from the possibility of theft or damage.

Procedure: Security of Equipment

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

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

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

- All valuable equipment should be marked using the appropriate identification method (ie. U V pen, Smartwater etc). Advice on this can be sought from the Security Team and IT helpdesk.

- Suspected thefts of equipment should be reported promptly to both the Head of Operations and Security Officer.

5.2. Security Hardware

Installation of CCTV, intruder alarms or access control systems on School property will only be undertaken following consultations with the Head of Operations who will advise on equipment, installers and security response. Where CCTV is installed, the requirements of the Data Protection Act must be adhered to.

5.3. Headed Paper and Stationery

Pre-printed headed paper and other stationery displaying the School logo, staff names, telephone numbers etc., must be treated carefully to avoid fraudulent use. Headed paper, order forms, compliment slips etc. should be locked away when not in use. Old or unwanted headed paper must be disposed of correctly by shredding.

5.4. Data Protection

The data of living persons is protected under the Data Protection Act. The Act creates responsibilities and rights in relation to all aspects of the collection, holding, use and disposal of personal data. Staff will want to handle personal data in an ethical way and the Act provides a framework for reaching this objective.

Staff should ensure that they are aware of School policy in this area and of the sources for further advice. FSB Data Protection Policy is published on the Staff Portal and Student Portal.

5.5. Protecting Information Assets

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

Damage of this type is not inevitable and by being aware of simple security measures and observing them, the chances of loss and damage can be minimised.

6. Asset Protection

6.1. Control of Cash

Cash from all sources throughout the School should be processed for collection by the School's appointed staff member.

Cash in excess of £50 is not to be held within Departments, overnight or at weekends, unless a suitable safe is available. Sums of £50 and less must be held in a locked drawer or cupboard and the key retained by a responsible person.

Safe keys should be the responsibility of a senior member of staff within the

Department, and should be taken home by a responsible member of staff, ensuring that appropriate arrangements are in place to cover holidays and sickness absence. The loss of such keys should be reported to the appropriate Senior Manager immediately.

Heads of Departments are responsible for maintaining proper security at all times for all buildings, stock, stores, furniture, equipment and cash under their control.

6.2. Prevention of Fraud

All enquiries relating to fraud should be directed to the CEO. Further action may be taken in line with the General Regulations and Procedures affecting Students or the School's Disciplinary Procedures.

6.3. Security in the Office

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.

Procedure: Office/Security

General Awareness:

- School ID cards should be carried by students and staff at all times on School premises.
- Students and staff should be aware of the procedure for reporting incidents.
- Staff working out of hours should ensure they follow 'out of hours' procedures and contact Security if they need assistance.

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

- Valuables and confidential documents (laptops, exam scripts, research data, personnel files etc) are locked away with keys secured in key cabinets or taken home:
- Any keys that have been issued during the day have been returned and any losses reported immediately.
- A 'clear desk policy' is maintained where possible to ensure confidential documentation is locked out of sight.
- All non-essential electrical appliances are switched off/unplugged.
- Doors and windows are closed and locked as appropriate.
- Ground floor curtains and blinds are closed with any items on windowsills, which hinder closure, removed and lights turned off.
- Intruder alarms (where installed and a local responsibility) are set.
- PC's are switched off or password protected when not in use to prevent unauthorised access to information.

6.4. Personal Security

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 School premises to take all reasonable measures to ensure their own personal security.

6.5. Suspicious Behaviour

If suspicious activity is noticed, individuals should notify, or get a colleague to notify the Security Staff. Challenge the behaviour if you feel able but do not get yourself into a

vulnerable or confrontational situation. More important is to make a mental or written note of a description, direction of travel, what suspicious acts you saw and any other information which may help Security identify and locate the individual(s). Security staff will direct security response to the area as a matter of urgency, and if appropriate, ensure the Police are contacted. Each situation of this type will be different, and it is at the discretion of the individuals concerned as to what action they wish to take, but at no time should they put themselves at risk.

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

6.6. Threatening or abusive behaviour

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

6.7. Drugs and Illegal Substances

All suspicions of the handling or using of controlled or illegal substances should be reported to the Head of Operations, in the first instance, so that appropriate investigation and consultation with School authorities may take place.

6.8. Property – Lost and Found

Found Property

Unidentified found property should be handed in to 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 is left unclaimed for a minimum of one month, the property will be passed to charity or disposed of.

Claiming Property

When a loser claims property, full details will be required. ie. a full description of the item and for certain items, proof of ownership may be requested. When staff are satisfied of the owner's claim, the property will be handed over on signature. Where any doubt to ownership exists, the Head of Operations or the local Police will be asked to arbitrate.

Property Left in Classrooms

No items of property or teaching material should be left unattended in teaching rooms. Teaching rooms are cleaned daily and any item of property will be treated as found property and dealt with as above. Where the value is questionable (leftover hand-outs or teaching material) and/or the condition of the item is poor, normal practice is to treat this as 'waste' and dispose of it.

Students' Property: General

The School does not accept liability for loss and/or damage to Students personal property unless negligence of the School or its employees can be established. Students are strongly advised to make their own arrangements for insuring their personal property.

7. Use of Closed-Circuit Television (CCTV)

7.1. Reasons for Use

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 School uses CCTV systems around the campus covering many of the vulnerable areas, public access points and adjacent streets. CCTV is installed, with the objective of assisting to provide a safe and secure environment for the benefit of those who work, live and visit the School. This objective will be met through the monitoring of the system so as to:

- Reduce the fear of crime and offer public reassurance for all students, staff and visitors to the campus.
- Assist in the detection, deterrence and prevention of crime on campus by securing evidence to identify, apprehend and prosecute offenders and to provide evidence for internal disciplinary hearings.
- Provide improved security of School property.

Appropriate signs will be placed around the School warning that CCTV is in use.

7.2. Locations

The School CCTV systems consist of both internal and externally located overt cameras with telemetry and digital recording (plus some video recording).

It is agreed that some departments e.g. Library Services, public computing rooms and the Students Union may benefit from a local CCTV system for the reasons described above. The operation of these systems and any future installations in departmental areas, must be authorised by the Head of Operations and comply with the Data Protection Act (DPA).

7.3. CCTV Operating Procedures

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

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

7.4. Police

In general, the Police should not require access to (nor be allowed access to) School CCTV systems except under the following circumstances:

- Emergencies or investigation of serious incidents
- Identification of offenders
- Liaison and training purposes, by prior arrangement with the Head of Operations
- As authorised by the Head of Operations

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

7.5. Recorded Images

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

7.6. Covert CCTV

This will not generally be used within the School but may be used in exceptional circumstances to assist in the detection of crime or apprehension of offenders. Before use, permission to use covert CCTV will be obtained through the HR Department and will be sited only for a time specific and necessary to the operation. Recordings from covert CCTV will be treated in accordance with the Data Protection Act.

More information on how the School uses CCTV can be found in the School's Policy and Standards for the Use of CCTV

8. Bomb Threats

Bomb threats can be received by telephone, by post, by e-mail or by directly placing a bomb in
or around a building. Alternatively, an item which cannot be identified, and which could contain a
bomb can be left. It may be a hoax or an innocent mistake but if in doubt, assume the worst.

Bombs may be disguised in many ways and are unlikely to look like a bomb.

Anyone one who receives a threat or has reason to believe a bomb is on the premises must immediately inform the Head of Operations or the nearest security staff member on duty; the Head of Operations will act as Emergency Co-ordinator. The Emergency Co-ordinator will summon the emergency services and arrange for the evacuation of the buildings.

8.1. Telephone Threat

The person who receives a telephone threat has a critical role to play. He/she may be able to
glean vital information. They must try to:

- Remain calm.
- Obtain as much information as possible by keeping the caller talking (e.g. make excuses like – 'it's a bad line'
- Send someone to summon a Senior Manager.

8.2. Bombs in the Post

If there is the slightest suspicion that a letter or package contains an explosive device**, it should not be moved,** and a marker should be placed next to it indicating that it is a suspicious package.

The following is a guide to identifying a dangerous item:

- The package feels heavier than would normally be expected,
- The person it is addressed to is not expecting it,
- Visible wiring or tin foil,
- Grease marks on the packaging,

8.3. Bomb Placed in Building

If a suspicious object is discovered, it must not be touched, and the finder should clear all persons away from the area and then send for or fetch a Senior Manager.

8.4. Procedure

Acting on the information received, the Emergency Co-ordinator will call the Emergency Services
unless on immediate inspection it is clear that the situation does not pose a risk.

The Emergency Co-ordinator will summon the Fire Marshals, who will undertake an orderly evacuation of the building. The Emergency Co-ordinator will arrange for the occupants of adjacent buildings to be informed.

The following must be observed:

- The Fire Alarm **must not** be activated,
- The use of all phones including mobiles must cease,
- All lights, electronic equipment etc. must be left as it is, i.e. nothing must be switched on or off.

8.5. **Basic Security**

Good housekeeping both inside and outside the building will reduce the opportunity for an explosive device to be planted. No packages, cases, bags etc should be left unattended in communal areas or in teaching rooms. Students should be warned that such items may be removed without warning and if subject to a security check damaged or destroyed. All deliveries must be made to a designated delivery point, at expected times during normal working hours and have delivery notes attached.

Version Tracking:

Version	Author / revisions by	Changes summary	Approved by	Date
1.0 – 2.0	Head of Assessments / Executive Committee	*Original version.*	Executive Committee	September 2017 August 2018 September 2019
2.1	Head of Operations Quality Audit Manager /	*Annual Review and update; formatting and addition of version control.*	Board of Governors	October 2020
2.2	Quality Audit	*Revision and removal of Covid 19 guidance.*	Board of Governors	November 2022