University of St Andrews

Security policy

Document type	**Policy**
Scope (applies to)	Public
Applicability date	26/06/2019
Review / Expiry date	09/09/2022
Approved date	23/12/2020
Approver	Director of Operations
Document owner	Business Manager
School / unit	Estates
Document status	Published
Information classification	Public
Equality impact assessment	27/06/2019
Key terms	Estate/Facilities management/Security
Purpose	This Policy will outline the approach of the University to ensure, as far as is reasonably practical, the personal safety and security of all students, staff, visitors and contributors across the University estate and University assets.

Contents Page

1.0 Purpose and Policy Statement

This Policy will outline the approach of the University to ensure, as far as is reasonably practical, the personal safety and security of all students, staff, visitors and contributors across the University estate and University assets, including all University controlled buildings.
This Policy does not cover Cyber Security related matters. These are addressed in 'Regulations governing the use of University ICT facilities' which can be found at https://www.st-andrews.ac.uk/media/it-services/policies-and-procedures/documents/regulations-acceptable-use-ict.pdf.

Responsibility for security and personal safety rests with all persons who study, work at, reside in or visit the University. All students, staff, visitors and contractors should assist University Security staff with physical security responsibilities in ensuring the success of the policy.

2.0 Scope

Physical security is an essential part of any security plan. It protects and preserves physical, human and information assets. The threats to these assets are usually natural disaster, vandalism, theft, sabotage, violence, catastrophes caused by human failure, accidental damage, terrorism and other non-traditional threats.

Providing Physical Security will involve a balance between physical presence and use of technology. The level of physical presence, e.g. patrols and guarding, is an ongoing evaluation/assessment and the use of technology will require constant monitoring to ensure it is working and operating as intended.

Physical Security requires appropriate 'layering' of physical and technical security such as appropriate building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, alarm systems and CCTV.

In general terms, physical security means the positioning of physical and procedural obstacles to prevent unauthorised access to buildings and other physical assets. This policy specifically addresses the responsibilities and governing framework for the management, installation and maintenance of the following:

- **Intruder Alarm Systems** including area surveillance sensors, infra-red devices, etc.
- **Access Control Systems** including door entry card systems, speed gates etc.
- **Closed Circuit Television (CCTV) Systems** including video surveillance, cameras, 360-degree surveillance domes, switching matrixes, IP video, digital recording, image analysis etc.

3.0 Legislation and Standards

Statutory and Common Law applicable to this physical security policy includes:

- Health and Safety at Work Act 1974
- Data Protection Act 2018
- EU GDPR
- Human Rights Act 1998
- Fire (Scotland) Act 2005
- Counter Terrorism and Security Act 2015

Standards applicable to the physical security policy include:

- BS7499:2013 Static Site Guarding and mobile patrol service – Code of Practice
- BS8495:2007 Code of Practice for digital CCTV recording systems for the purpose of image export to be used as evidence
- BS7958:2015 Closed Circuit Television (CCTV) Management and Operation – Code of Practice
- BSRIA FMS 3/98 "Standard Specification for Electronic Security Systems" Building Services Research and Information Association (BSRIA)

4.0 Responsibilities:

Shared responsibility for security rests with **all** students, staff and visitors to the University. In particular, everyone should report all activity, suspected or real, of a criminal nature or any suspicious activity immediately to the Security and Response Team. It may also be necessary to ensure the Police are alerted.

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

a) Security Strategy Group (SSG): The SSG is chaired by the Vice Principal (Governance) and reports to the Risk Management Group (RMG). The SSG is formed to set direction and advise the University Senior Management in relation to security-related matters, prioritise security-related developmental improvement, propose and oversee security-related projects (where appropriate) and generally oversee the security of University assets in a consistent fashion through one consistent route. This is achieved as part of an overarching physical security policy to continuously and proactively enhance the safety and security of staff, students, visitors and the community. The strategic endorsement and prioritisation management of security-related issues across the University and associated resources will be co-ordinated through the SSG. The SSG will approve the Security Policy and ensure that support and resources are available to staff for the implementation of the Policy. Necessary measures to improve security in essential areas will receive priority consideration. Where appropriate, specific training to achieve acceptable standards of operation will be supported and properly resourced.

b) Head of Estates (delegated to the University Security Manager): overall development, planning and implementation of physical security procedures and the monitoring of their effectiveness and efficiency. Investigation of breaches in physical security and related

crimes; liaison with police, emergency services and local authorities; monitoring and management of intruder alarms, access control and CCTV systems.

c) Estates and Buildings: training of estates staff in physical security issues; installation and maintenance of intruder alarm, CCTV and access control systems agreed with IT Services. Procure and communicate contracted suppliers and systems.

d) IT Services; training of IT staff in physical, including cyber, security issues; installation, maintenance and contract management of access control software and IT hardware including log of repairs. Provide asset register of all maintained access control systems. Procure and communicate with contracted suppliers and systems.

e) Data Protection and Freedom of Information Office: Advise and liaise with Security regarding intruder alarm, access control and CCTV specifications and related signage, ensuring compliance with DPA. Contribute to the University's CCTV Code of Practice.

f) Heads of Schools and Professional Services Directors: have a key role in promoting security within their buildings. The actual responsibilities will vary according to the location and the nature of the activity taking place. A number of specific responsibilities can be identified:

- Liaise with the University Security Manager on any security matter as required.
- Ensuring their staff have access to and are familiar with the Security Policy, paying particular attention to those issues which are directly relevant to their activities.
- Ensuring that all members of staff and students in their buildings understand and exercise their physical security responsibilities, including the displaying of University Identity Cards when appropriate, and have due regard to University property.
- Control access to their buildings by approving the issue of keys / access control cards and by authorising staff to have 'out of hours access' only as necessary.
- Notifying Security and Response Team staff of any physical security risk (including the purchase of expensive equipment etc.) to enable advice on any additional physical security or protection.
- Ensure that there is no installation of intruder, access control and CCTV systems without prior approval of the University Security Manager.
- Keep a record of all keys / access cards issued locally and ensure that staff return keys when they move offices or leave the University's employment. (Nb. 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.)

g) Staff: All staff must ensure they are familiar with and follow the procedures in the University Security Policy, paying particular attention to those issues which are relevant to their activities. They must also co-operate with requests from Security and Response Team staff, especially in emergency or evacuation situations and in relation to physical security procedures. Staff are encouraged to display their University identity cards at all times when on University property.

h) Students: have a general responsibility to look after University facilities properly and to give due consideration to physical security issues. They must follow security procedures designed to protect University property, in particular regulations governing access to computer rooms or areas with other open use equipment.

Students must co-operate with requests from Security and Response Team staff, especially in emergency or evacuation situations and in relation to physical security procedures. Students are encouraged to display their University identity cards at all times when on University property

Students who are residents in University Managed Halls or Halls managed by external organisations should follow the halls of residence procedures (which include security instructions) issued to Students by Residential Services and the Management of the externally operated halls.

i) Visitors: (including conference delegates and external event attendees) have a general responsibility to look after the University facilities whilst on campus and to give due consideration to physical security issues. In particular they must follow security procedures designed to protect University property and where issued, wear their visitors badge at all times. Visitors must follow instructions from the Security and Response Team staff or from their host College, School or Service, particularly in emergency situations.

5.0 Policy Implementation

The University will adopt a layered approach to security and will:

5.1 Where and when deemed appropriate, secure the perimeters of its buildings by taking all reasonable measures to prevent unauthorised access.

5.2 Reserve the right to limit access to its buildings to students, staff, visitors, clients and contractors.

5.3 Take additional security measures to protect its high value assets, high-risk facilities and confidential documentation storage areas.

5.4 Provide additional security measures to ensure the protection of staff and equipment. These measures include, where applicable: -

5.4.1 The provision of digital locks on doors where necessary.

5.4.2 The requirement for all IT equipment to be marked with a unique identification code and all servers to be installed in secure locations.

5.4.3 Liaison with staff who work offsite to ensure appropriate measures are taken to minimise the risk to their personal safety and the security of any equipment being transported.

5.5 Provide a range of Personal Protection Security measures for those staff that work in high-risk situations. These measures may include: -

5.5.1 The introduction and operation of CCTV surveillance in sensitive or higher risk areas in or around the University estate as agreed in conjunction with the SSG and the University's CCTV Code of Practice.

5.5.2 The provision of security patrols

5.5.3 Personal (panic) alarm systems at strategic and higher risk locations or on person

5.6 The University will, in utilising these measures, ensure full compliance with The Data Protection Act 2018, EU GDPR and any relevant University Codes of Practice and revisions thereof.

5.7 The University will employ Security staff who are appropriately trained.

5.8 The University will employ Security staff who are trained and authorised to operate and monitor CCTV equipment, where necessary.

5.9 To ensure uniformity of standards, fitness for purpose and to limit costs, the University will where appropriate adopt standard specifications for the following items of security equipment:

- Intruder Alarm Equipment
- Access Control Systems including Identity Cards
- CCTV surveillance and CCTV recording equipment
- Door furniture, locks and suiting
- Digital Locks
- Security Lighting

5.11 The University in pursuance of the purpose of this policy will:

5.11.1 Reserve the right to conduct spot checks to ensure that individuals in the University can provide evidence that they are genuine learners, staff, visitors or contractors to the premises.

5.11.2 Reserve the right to require individuals who cannot provide evidence that they are genuine students, staff, or visitors to leave the premises.

5.11.3 Request police assistance in the event of any criminal offence being committed on University property.

5.11.4 Provide advice to students and staff on personal safety and the security of items and equipment.

5.11.5 Provide adequate lighting in and around University buildings such as car parks and access routes.

5.12 The University layered approach will be generally defined as follows;

The grounds of the University will be generally open with certain restrictions as is appropriate to the use and contents of buildings on the University estate.

The external faces of all University buildings should, where necessary, have a minimum of two means of security. In practice this will mean locks on doors and windows along with a suitable and efficient intruder alarm system to be utilised when the building is not in use. There will be buildings on the University estate which will require additional or replacement measures such as the focussed use of monitored CCTV and Security and Response Team and Janitorial checks to physically test that buildings are secure.

Internally buildings should have easy open access to public areas as appropriate.

Access from open areas to secure areas within a building should be incremental and appropriate to the use, contents and sensitivity of the area to be protected. A form of Threat

and Risk Assessment process should be carried out in which building users and other interested parties may raise issues, concerns, threats, challenges etc. to provide an informed basis for decision making.

There will be areas where it is important to restrict and control access. It may be relevant to consider input from external bodies to ensure compliance with national standards. This will include the Home Office for the storage and secure management of controlled drugs or the Police Counter Terrorism and Security Advisor in relation to sensitive laboratory areas.

6.0 Intruder Alarms and Access Control Systems

Intruder Alarms and Access Control Systems operate in some areas. Card controlled barriers/doors are an effective method of preventing unauthorised access and the security strategy will involve expansion of access control systems throughout the University. Access cards should be regarded for security purposes as the same as a key. Cardholders must safeguard their card and report any loss to Campus Card Services and the Security and Response Team as soon as possible, so the card access can be cancelled.

7.0 Closed Circuit Television (CCTV) Systems

The University has a CCTV Code of Practice which details the management and operations, storing and viewing of images, disclosure and retention of recorded images amongst other related matters. A copy of the Code of Practice can be obtained from the University website.

8.0 Monitoring and Evaluation

Responsibility for monitoring and evaluation of the University Security Policy lies with the SSG and the University Security Manager. The policy will be reviewed every two years or when any new legislation or statutory obligations arise as identified by the SSG.

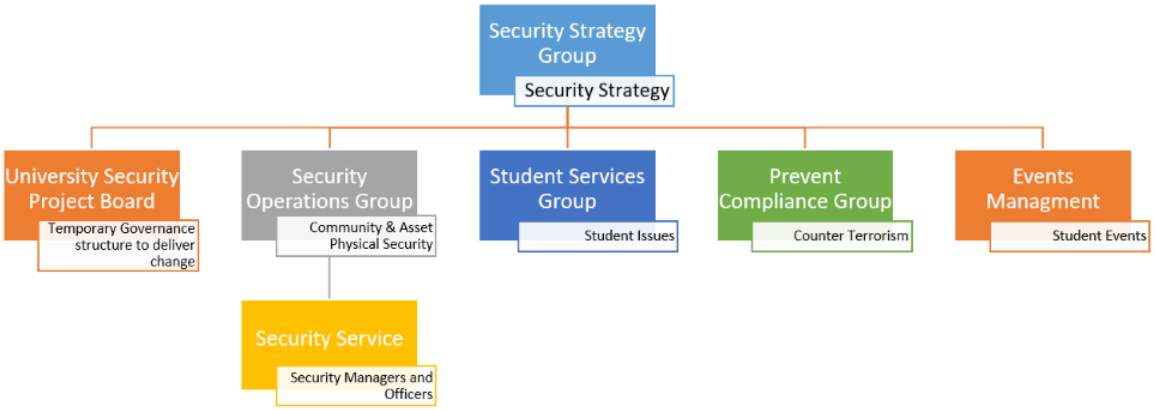
9.0 Related Policies and Further References

- CCTV Code of Practice
- Health and Safety Policy
- Counter Terrorism Protective Security Advice for Higher and Further Education(2009) *National Counter Terrorism Security Office (NacTSO)*

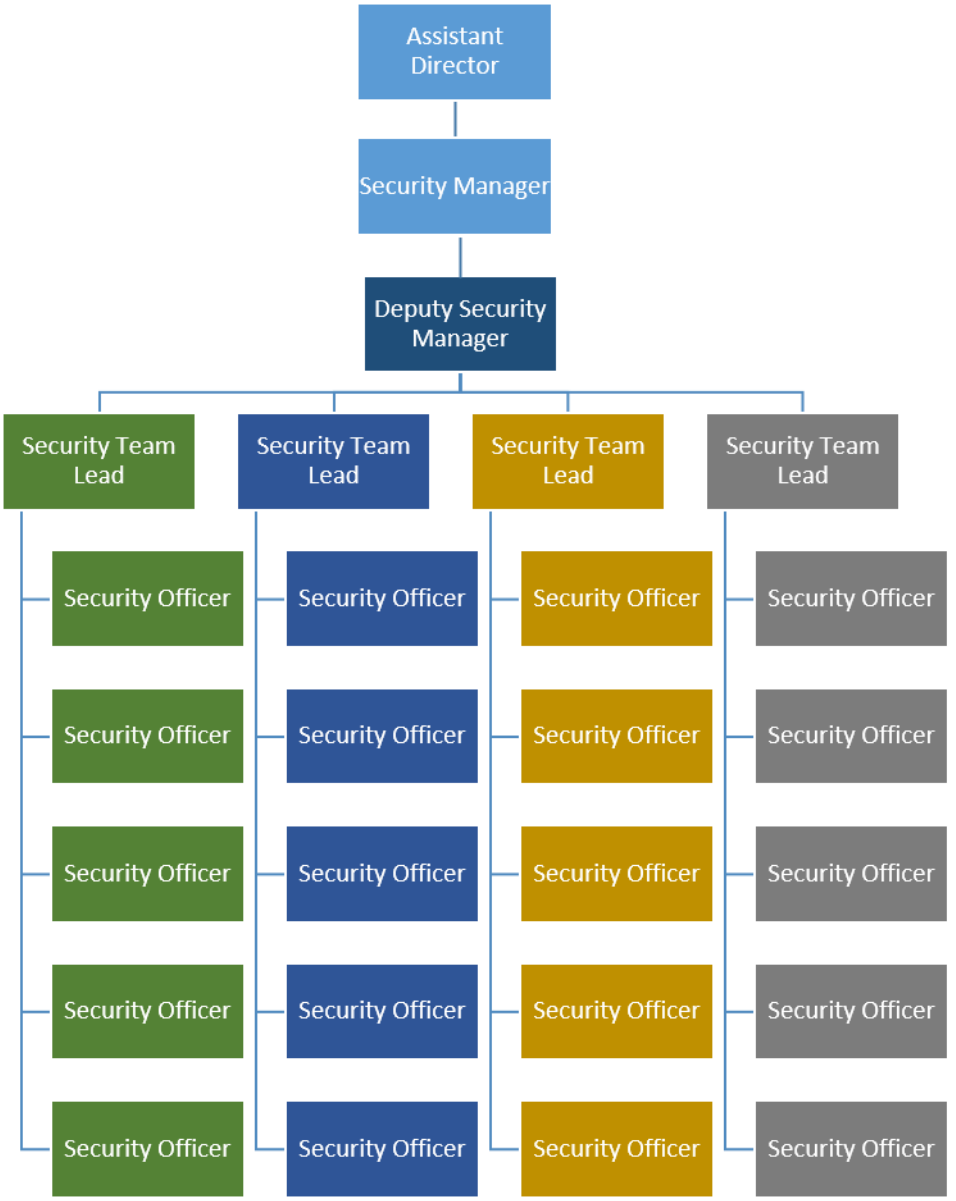
10 Glossary of Terms

BS – Relates to relevant guidance produced by the British Standards Institution
CCTV – Closed Circuit Television system(s)
DPA – Data Protection Act 2018
EU GDPR – European Union General Data Protection Regulation
IP video – internet protocol video
NacTSO – National Counter Terrorism Security Office
RMG – University Risk Management Group
SSG – University Security Strategy Group
Please see below organograms for visual representation of the Security Governance Framework in place at the University and also the Security Operating Model.

Security Governance Framework



Security Operating Model



Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
2.0	Amendment	Submitted	A Edmonston	22/12/2020