

SECURITY POLICY

V1.0

Policies superseded by this version

This document replaces the 2 individual existing Security policies from legacy City and St Georges organisations.

Summary of changes to previous version

The policy has not materially changed the operational purpose of the University's Security strategy but has been reformatted to separate governance requirements from operational procedures. Existing responsibilities, legislative requirements and operational controls have been consolidated to improve clarity and support consistent implementation across all campuses. There is now also further focus on emergency response and security preparedness in anticipation of the Terrorism (Protection of Premises) act 2025 preparedness plan

Table of contents

Section:	Heading:	Page number:
1	Introduction	1
2	Freedom of speech and academic freedom	2
3	Equity, Diversity and Inclusion	3
4	Definitions	3
5	Policy	5
6	Procedure	8
7	Advice and guidance	29
8	Failure to comply	31
9	Review	31
	Appendices	

1 Introduction

City St George's, University of London is committed to providing a safe, secure and inclusive environment that enables students, staff, contractors, visitors and partners to study, work, teach, undertake research and access University services safely.

Security is fundamental to the University's ability to deliver its academic mission and protect its people, information, assets and reputation. Effective security arrangements support teaching, research, healthcare partnerships, public engagement and business continuity whilst ensuring that the University remains an open and welcoming institution.

The University recognises that the security risk landscape continues to evolve and includes threats arising from crime, anti-social behaviour, terrorism, hostile acts, cyber-enabled physical attacks, insider threats and other disruptive activity. The University therefore adopts a proportionate, intelligence-led

and risk-based approach to physical security that balances openness with the need to protect people, property and critical infrastructure.

Policy Objectives

This policy aims to:

- Provide a clear framework for the management of physical security across the University;
- Define the responsibilities of staff, students, contractors and visitors in maintaining a secure environment;
- Establish consistent standards for the protection of people, property, information and infrastructure;
- Support the prevention, detection and investigation of crime and security incidents;
- Provide arrangements for access control, incident reporting and asset protection;
- Strengthen preparedness for emergencies, major incidents and acts of terrorism;
- Ensure compliance with applicable legislation and recognised good practice;
- Support continuous improvement through monitoring, assurance and regular review.

Security is a shared responsibility and everyone who uses University premises has a role in maintaining a safe and secure environment.

This policy establishes the governance framework for the management of physical security across all University campuses and applies to everyone who studies, works or visits the University.

The policy should be read alongside associated University policies, standards and procedures relating to health and safety, information security, data protection, emergency management, business continuity and counter terrorism.

Strategic Context

This policy supports the University's wider commitment to governance, health and safety, resilience and organisational risk management.

It forms part of the University's integrated approach to protective security and contributes to compliance with relevant legislation, regulatory requirements and recognised good practice.

The policy supports the University's preparedness under the Terrorism (Protection of Premises) Act 2025 (Martyn's Law) by establishing clear governance arrangements, defined responsibilities and operational procedures for the management of security risks.

The University adopts a risk-based approach to protective security that reflects the nature of its campuses, the diversity of its activities and the expectations placed upon modern higher education institutions. This includes maintaining effective relationships with the emergency services, local authorities, the police, the National Protective Security Authority (NPSA), ProtectUK and other relevant partners where appropriate.

Nothing within this policy replaces an individual's responsibility to exercise reasonable care for their own safety or the safety of others. Rather, the policy establishes the framework within which security arrangements are managed and coordinated across the University.

2 Freedom of Speech and Academic Freedom

- 2.1 City St George's, University of London, regards freedom of speech and academic freedom to be fundamental to delivering its mission as the University of business, practice and the professions. Its

values in this respect are set out in a code of practice on freedom of speech and academic freedom, which explains how the University will uphold, secure, and promote freedom of speech within the law: <https://www.citystgeorges.ac.uk/about/governance/policies/code-of-practice-on-freedom-of-speech>.

- 2.2 Nothing in this policy should be interpreted in any way that would be inconsistent with the code of practice and – in the event of any inconsistency – the provisions of the code will prevail.

3 Equity, Diversity and Inclusion

- 3.1 City St George's, University of London works to advance equity, diversity and inclusion in its activities, processes, and culture, for the whole University community, including staff, students and visitors.
- 3.2 The University will meet its obligations under the Equality Act 2010 in its policies and seek to eliminate discrimination on the basis of age, caring responsibilities, disability, gender identity, gender reassignment, marital status, neurodiversity, pregnancy, race, religion or belief, sex, sexual orientation, and socio-economic background.

4 Definitions

- 4.1 **Access Control** - The measures, systems and procedures implemented by the University to regulate and control access to buildings, rooms, facilities and other restricted areas, including electronic access control systems, mechanical locks, keys and identification cards.
- 4.2 **Authorised Person** - An employee, contractor or other individual acting on behalf of City St George's, University of London who has been granted permission to undertake specific security-related duties or access designated areas in connection with their role.
- 4.3 **Contractor** - Any individual or organisation engaged by the University to undertake work or provide services on University premises, whether directly employed by the University or through a third-party provider.
- 4.4 **Identification Card** - An official University-issued identification card that provides proof of identity and, where authorised, enables electronic access to University buildings and facilities.]
- 4.5 **Out-of-Hours Access** - Access to University premises outside published opening hours or normal operational periods, which may require additional authorisation and security controls.
- 4.6 **Physical Security** -The combination of personnel, procedures, physical measures and security systems designed to protect people, buildings, information, equipment and other University assets from loss, damage or unauthorised access.
- 4.7 **Restricted Area** - Any location within the University estate where access is controlled because of operational, security, research, legal or safety requirements.

Restricted areas may include laboratories, data centres, plant rooms, security control rooms, clinical environments, hazardous storage areas and other locations designated by the University

- 4.8 **Security Incident** - Any event, act or circumstance that threatens, or has the potential to threaten, the safety of individuals, the security of University property or the continuity of University operations.

Security incidents include, but are not limited to:

- Theft
- Criminal damage;
- Unauthorised access;
- Assault;
- Abusive or threatening behaviour;
- Suspicious activity;
- Loss of security equipment or keys;
- Terrorism-related incidents;
- Malicious acts;
- Significant security system failures.

- 4.9 **Security Control Room** - A designated University facility from which security systems are monitored, incidents are managed and emergency responses are coordinated.
- 4.10 **Security Officer** - A member of the University's Security Team or an authorised security contractor responsible for protecting people, property and assets, responding to incidents and enforcing University security procedures
- 4.11 **Protective Security** - The application of physical, personnel and procedural security measures designed to reduce the likelihood and impact of hostile acts, criminal activity, terrorism and other threats affecting the University
- 4.12 **Visitor** - Any individual attending University premises who is not a current student, member of staff or authorised contractor.
- 4.13 **Counter Terrorism** - The policies, procedures and protective security measures implemented by the University to reduce the risk from terrorism and to support compliance with the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), associated statutory guidance and recognised good practice.
- 4.14 **University Property** - All buildings, land, equipment, information, vehicles, infrastructure and other assets owned, leased, managed or otherwise under the control of City St George's, University of London.
- 4.15 **University Community** - All staff, students, contractors, agency workers, volunteers, visitors, researchers, honorary staff and any other persons who access or use University premises or services.

5 Policy

5.1 Scope

This policy applies to all members of the University community, including staff, students, contractors, agency workers, volunteers, honorary staff, consultants, visitors and any other persons accessing or undertaking activities on University premises.

The policy applies to all buildings, campuses, residences (where managed by the University), land, infrastructure, vehicles, equipment and other assets owned, leased, managed or otherwise under the control of City St George's, University of London.

The requirements of this policy apply to all activities undertaken on behalf of the University where physical security arrangements are required, including teaching, research, commercial activities, public events and collaborative working with partner organisations.

This policy should be read alongside the University's Health and Safety Policy, Fire Safety Policy, Information Security Policy, Data Protection Policy, Business Continuity Framework, Emergency Management arrangements and associated Security Procedures.

5.2 Security Principles

The University is committed to maintaining a safe, secure and welcoming environment whilst supporting openness, accessibility and academic freedom.

The University's approach to physical security is based upon the following principles.

Risk-Based Security

Security measures shall be proportionate to the risks identified through ongoing threat, vulnerability and risk assessments.

Protective security measures shall be regularly reviewed to ensure they remain appropriate, effective and proportionate.

Shared Responsibility

Security is everyone's responsibility.

All members of the University community are expected to remain vigilant, report security concerns promptly and comply with University security arrangements.

Prevention

The University will seek to prevent incidents wherever reasonably practicable through effective planning, security awareness, appropriate physical security measures, access control, surveillance and partnership working.

Preparedness

The University shall maintain appropriate plans, procedures, training and exercising arrangements to ensure an effective response to security incidents, major emergencies and acts of terrorism.

Partnership

The University will maintain effective working relationships with the Metropolitan Police Service, London Fire Brigade, London Ambulance Service, NHS partners, local authorities, ProtectUK, the National Protective Security Authority (NPSA) and other relevant agencies where appropriate.

Continuous Improvement

Security arrangements shall be reviewed regularly to identify opportunities for improvement, respond to changes in threat and ensure compliance with legislation and recognised good practice.

5.3 Roles and responsibilities

University Executive

The University Executive has overall responsibility for ensuring appropriate governance arrangements exist to support the safety and security of the University community.

The Executive shall ensure that sufficient resources are made available to implement this policy effectively.

Assistant Director – Facilities Management

The Assistant Director – Facilities Management is accountable for the strategic oversight of physical security across the University and for ensuring that appropriate governance arrangements remain in place.

Head of Security

The Head of Security is responsible for the development, implementation and continuous improvement of the University's physical security arrangements.

Responsibilities include:

- Developing security strategy, policy and standards;
- Managing operational security services;
- Overseeing security risk assessments;
- Ensuring compliance with relevant legislation;
- Managing security systems and technologies;
- Overseeing incident reporting and investigation;
- Maintaining relationships with emergency services and external partners;
- Leading the University's protective security and counter terrorism arrangements;
- Ensuring appropriate training and awareness programmes are delivered;
- Providing assurance to senior management regarding the effectiveness of security arrangements.

Managers

Managers are responsible for ensuring that appropriate security arrangements are implemented within their areas of responsibility.

They shall:

- Ensure staff understand local security procedures;
- Report security risks and incidents;
- Support investigations where appropriate;
- Ensure security equipment is used correctly;
- Notify Security of significant operational changes that may affect security.

Staff and Students

Every member of the University community has a responsibility to contribute to a safe and secure environment.

Individuals are expected to:

- Comply with this policy and associated procedures;
- Challenge or report suspicious behaviour where appropriate;
- Safeguard University property;
- Protect University identification cards, keys and access credentials;

- Report security incidents promptly;
- Cooperate with Security staff during incidents and emergencies.

Security Team

The Security Team is responsible for delivering the University's operational security service.

This includes:

- Responding to incidents;
- Patrolling University premises;
- Monitoring security systems;
- Managing access control;
- Supporting emergency response;
- Investigating security incidents;
- Providing security advice;
- Protecting people and property;
- Supporting business continuity arrangements.

5.4 Legislative and Regulatory Compliance

The University shall operate its security arrangements in accordance with all applicable legislation, statutory duties and recognised good practice.

This includes, but is not limited to:

- Health and Safety at Work etc. Act 1974;
- Occupiers' Liability Acts 1957 and 1984;
- Human Rights Act 1998;
- Data Protection Act 2018;
- UK General Data Protection Regulation (UK GDPR);
- Regulatory Reform (Fire Safety) Order 2005;
- Terrorism (Protection of Premises) Act 2025 (Martyn's Law);
- Private Security Industry Act 2001;
- Equality Act 2010;
- Civil Contingencies Act 2004;
- applicable Home Office, ProtectUK and National Protective Security Authority (NPSA) guidance.

5.5 Governance, Monitoring and Assurance

The University shall maintain appropriate governance arrangements to ensure that physical security remains effective, proportionate and aligned with organisational risk.

The Head of Security shall establish arrangements for:

- Regular security risk assessments;
- Periodic review of physical security measures;
- Monitoring security incidents and trends;
- Audit of access control systems and security processes;
- Review of counter terrorism preparedness;
- Monitoring compliance with this policy;
- Annual reporting on security performance;

- Review of lessons identified following incidents, exercises and audits.

Security arrangements shall be reviewed whenever there are significant changes to legislation, the threat environment, University operations, organisational structure or the physical estate.

The findings of audits, inspections, incident investigations and operational debriefs shall be used to inform continuous improvement and future revisions of this policy.

6 Procedure

6.1 Security Management Framework

The University maintains an integrated physical security service designed to protect people, property, information and operations across all campuses.

Security services are delivered through a combination of appropriately trained Security Officers, Security Supervisors, Security Managers, electronic security systems and established operating procedures.

The Security Team operates on behalf of the University to:

- Maintain a safe and secure environment;
- Provide a visible security presence;
- Respond to emergencies and security incidents;
- Investigate reported incidents where appropriate;
- Manage access to University premises;
- Protect University assets;
- Support students, staff and visitors;
- Work collaboratively with emergency services and partner organisations.

Security arrangements shall be proportionate to the level of risk presented by each campus, building or activity and shall be reviewed periodically to ensure they remain effective.

6.2 Security Incident Reporting

All members of the University community have a responsibility to report security concerns, suspicious behaviour, criminal activity, safety concerns or security incidents as soon as reasonably practicable.

Security incidents should be reported immediately to the Security Control Room or Security Team using the following reporting arrangements:

0207 840 3333 (internal ext. 3333) (Security control, Clerkenwell & Moorgate – University building 1st floor) Email Security@citystgeorges.ac.uk

Or **0208 7250044** (Tooting – Hunter wing Control room). Email sgul-security@sgul.ac.uk

Both locations are manned 24 hours.

All pertinent information should be included - time, location, persons involved, items missing, witnesses etc.

Examples of reportable incidents include, but are not limited to:

- Theft;
- Attempted theft;
- Criminal damage;
- Assault;
- Abusive or threatening behaviour;
- Unauthorised access;
- Suspicious persons or activity;
- Missing or stolen identification cards;
- Missing keys;
- Suspicious packages or vehicles;
- Terrorism-related concerns;
- Security system failures.

The Security Team shall assess each report, determine an appropriate response and record the incident in the University's incident management system.

Where necessary, Security shall notify the Police, emergency services or other relevant authorities. Serious incidents shall be escalated in accordance with the University's Major Incident Management arrangements.

6.3 **Emergency Response**

Security personnel shall provide an immediate response to security-related emergencies occurring on University premises.

The Security Team shall:

- Attend reported incidents;
- Assess immediate risks;
- Protect life where reasonably practicable;
- Preserve scenes where criminal offences may have occurred;
- Coordinate with emergency services;
- Assist evacuation or lockdown procedures where required;
- Support business continuity and recovery activities following incidents.

Where incidents involve violence, terrorism, hazardous materials or other significant risks, Security personnel shall follow the University's emergency procedures and any relevant operational plans.

Security staff shall not place themselves or others at unnecessary risk and shall always act within the limits of their training and competence.

6.4 **Access control and University Identification Cards**

The University operates electronic and physical access control systems to protect people, buildings, information and assets. Access to University buildings shall be based upon operational need and the principle of least privilege.

University Identification Cards remain the property of the University and shall be issued in accordance with approved procedures.

Identification cards shall:

- Be worn or visibly on display whilst on University premises;
- not be shared or loaned to another individual;
- be produced upon request by authorised members of staff;
- be reported immediately if lost, stolen or damaged.

Access permissions shall be granted according to an individual's role and operational requirements.

Managers are responsible for notifying Security of changes affecting access permissions, including new starters, changes of role and leavers. Access rights shall be reviewed periodically to ensure that permissions remain appropriate.

Any misuse of University Identification Cards or deliberate attempts to circumvent access control arrangements may result in disciplinary action and withdrawal of access privileges.

The University reserves the right to suspend or withdraw access where this is necessary to protect the safety and security of individuals, University property or operations.

Access arrangements may vary between University campuses to reflect differences in operational requirements, clinical environments, research activities, shared premises, opening hours and local security risks. Campus-specific procedures and local operating arrangements may be implemented where necessary, provided they remain consistent with the principles and governance requirements set out in this policy.

6.5 Contractors, Visitors and Out-of-Hours Access

The University is committed to maintaining a secure environment whilst ensuring that contractors, visitors and authorised persons can access its campuses safely and efficiently.

Appropriate arrangements shall be implemented to manage access by individuals who are not routinely based within the University and by members of the University community requiring access outside normal operating hours.

Contractors

All contractors undertaking work on University premises shall comply with the University's security arrangements, local site rules and any instructions issued by authorised University personnel.

Where appropriate, contractors shall:

- Sign in and out using the University's approved visitor management system;
- Display an authorised visitor or contractor pass at all times whilst on University premises;
- Remain within authorised areas relevant to their work;
- Comply with access restrictions applicable to sensitive or restricted areas;
- Report security concerns, suspicious activity or incidents immediately to the Security Team;
- Return visitor passes or temporary access credentials upon completion of their visit.

Contractors undertaking works within high-security, clinical, research or other restricted environments may be subject to additional access controls, supervision or permit arrangements.

Managers responsible for commissioning contractors shall ensure that appropriate security requirements are communicated before work commences.

Visitors

Visitors are welcome across the University's campuses; however, appropriate measures shall be implemented to safeguard the security of the University community and its assets.

Visitors shall normally:

- Register through the University's approved visitor management process where applicable;
- Be issued with an appropriate visitor pass where required;
- Comply with reasonable instructions issued by Security personnel or University staff;
- Remain within authorised areas;
- Be accompanied where required by the host department or authorised representative.

Departments hosting visitors remain responsible for ensuring that appropriate arrangements are in place for their reception, supervision and departure where necessary.

The University reserves the right to refuse entry to, or require the removal of, any visitor whose behaviour presents a risk to the safety, security or wellbeing of others or who fails to comply with University policies or reasonable instructions.

Out of Hours Access

The University recognises that certain teaching, research, operational and support activities may require access to University premises outside published opening hours. Out-of-hours access shall only be granted where there is a legitimate operational, academic or business requirement.

Access permissions shall be approved in accordance with local procedures and shall be limited to the minimum areas and duration necessary.

Individuals accessing University premises outside normal operating hours shall:

- Carry a valid University identification card or authorised access credential;
- Comply with all University security procedures;
- Ensure that doors, windows and other security measures remain secure upon entering and leaving buildings;
- Report any suspicious activity, faults or security concerns immediately;
- Cooperate with Security personnel undertaking patrols or access verification.

The University reserves the right to withdraw out-of-hours access where operational requirements change, where access is no longer required or where misuse of access privileges is identified.

Access to laboratories, workshops, clinical facilities, hazardous environments or other designated high-risk areas outside normal operating hours may be subject to additional authorisation, risk assessment or local management controls.

Security personnel may challenge any individual found on University premises outside normal operating hours to confirm their identity and authority to be present. Individuals are expected to cooperate fully with such requests.

Where necessary to protect life, property or the security of the University, Security personnel may refuse access to buildings or require individuals to leave areas where there is an identified safety or security risk.

6.6 Keys, Locks and Physical Security

The University maintains a range of physical security measures to protect people, buildings, information, equipment and other assets from unauthorised access, theft, damage or misuse.

These measures include, but are not limited to, mechanical locking systems, electronic access control systems, security glazing, intruder alarms, CCTV, perimeter protection and other physical security measures proportionate to the level of identified risk.

Keys

University keys remain the property of City St George's, University of London at all times. The issue, control, storage and return of keys shall be managed in accordance with the University's approved key management procedures.

Individuals issued with University keys are responsible for ensuring that they are:

- Kept secure at all times;
- Not loaned or transferred to another person without authorisation;
- Not duplicated without the University's written approval;
- Returned immediately when no longer required or upon leaving the University.

Any lost, stolen or unaccounted-for key shall be reported immediately to the Security Team. The University reserves the right to recover the cost of replacement keys, locks or associated security measures where loss results from negligence or unauthorised use.

The management of electronic access credentials is addressed in section 6.4 of this policy.

Locks and Physical Security

Building managers and departments shall ensure that offices, teaching spaces, laboratories, stores and other accommodation are secured whenever left unattended.

Doors fitted with electronic access control systems shall not be wedged or otherwise prevented from operating correctly except where authorised for operational purposes.

Fire doors shall not be secured in a manner that compromises their intended fire safety function.

Where physical security defects are identified, including damaged locks, defective doors, broken windows or compromised access control arrangements, these shall be reported immediately through the University's approved maintenance reporting procedures.

Temporary security measures may be implemented by the Security Team where necessary until permanent repairs have been completed.

Restricted Areas

Access to restricted areas shall be limited to authorised persons whose duties require entry.

Examples of restricted areas include:

- Security Control Rooms;
- Data centres and communications rooms;
- Plant rooms;

- Clinical environments;
- Laboratories;
- Engineering spaces;
- Hazardous storage areas;
- Cash handling locations;
- Areas designated as critical infrastructure.

Managers responsible for restricted areas shall ensure that access permissions are reviewed regularly and withdrawn promptly where operational requirements change.

Security of Premises

Before leaving University accommodation, staff shall take reasonable steps to ensure that:

- Doors and windows are secured;
- Confidential information is protected;
- Valuable equipment is stored securely;
- Alarms are set where appropriate;
- Unauthorised persons are not permitted to remain within the premises.

The Security Team may carry out periodic inspections of University premises outside normal operating hours to identify insecure buildings, defective security measures or other vulnerabilities requiring remedial action.

6.7 Asset Protection

City St George's, University of London is committed to protecting its physical, financial, technological and intellectual assets from loss, theft, damage, misuse and unauthorised access. Asset protection is a shared responsibility. All members of the University community are expected to take reasonable steps to safeguard University property and to report any concerns promptly.

General Responsibilities

Staff, students and other authorised users shall take appropriate measures to protect University assets under their control.

This includes ensuring that:

- Offices, teaching rooms and laboratories are secured when left unattended;
- Valuable equipment is not left unsecured in public or accessible areas;
- Portable devices are stored securely when not in use;
- University property is used only for legitimate University purposes;
- Security incidents, theft, damage or attempted theft are reported immediately.

Individuals are expected to exercise reasonable care in protecting University assets and shall not deliberately or recklessly expose property to unnecessary risk.

High Value Equipment

Equipment identified as being of significant financial, operational or research value shall be subject to additional security measures appropriate to the level of identified risk.

These measures may include:

- Secure storage;
- Electronic access controls;
- CCTV coverage;
- Asset marking or tracking;
- Alarm protection;
- Restricted access arrangements;
- Enhanced inventory management.

Heads of Department are responsible for ensuring that appropriate local arrangements exist for the protection of specialist equipment within their areas of responsibility.

Research, Clinical and Specialist Assets

The University recognises that certain research, clinical and specialist assets require enhanced protection because of their financial value, regulatory requirements or critical importance to teaching, research or healthcare activities.

Security measures for these areas shall be determined through appropriate risk assessment and may include additional physical security measures, restricted access, enhanced monitoring and local operating procedures.

Departments responsible for specialist facilities shall work with the Head of Security to ensure that appropriate protective security arrangements are maintained.

Information and Documentation

Although the management of information security is addressed within separate University policies, staff shall ensure that confidential documents, examination materials, research information and sensitive records are protected from unauthorised access whilst on University premises.

Where confidential information is no longer required, it shall be disposed of using the University's approved confidential waste arrangements.

Personal Property

The University accepts no liability for the loss of, or damage to, personal property unless liability arises through negligence on the part of the University.

Members of the University community are encouraged to take reasonable precautions to safeguard their personal belongings and should avoid leaving valuable items unattended.

Where facilities are provided for the secure storage of personal property, individuals are expected to make appropriate use of them.

Reporting Loss or Damage

Any loss, theft, attempted theft, criminal damage or suspected malicious activity affecting University property shall be reported immediately to the Security Team.

Where appropriate, Security shall investigate the incident and determine whether referral to the Police, insurers or other relevant authorities is required.

Departments shall cooperate fully with investigations and provide any information necessary to support recovery, insurance claims or criminal proceedings.

Lessons identified following incidents involving theft, criminal damage or asset loss shall be used to improve physical security measures, procedures and risk management arrangements across the University.

Shared Premises and Partner Organisations

The University occupies and operates within a number of locations where buildings, facilities or infrastructure are shared with partner organisations, including NHS organisations and other external stakeholders.

Where security responsibilities are shared, the University shall work collaboratively with partner organisations to ensure that appropriate security arrangements are established, maintained and regularly reviewed.

Departments operating within shared premises shall ensure that local security responsibilities, emergency procedures and reporting arrangements are clearly defined and communicated to staff, students, contractors and visitors.

Where security risks extend beyond the University's direct control, the Head of Security shall maintain appropriate liaison with partner organisations to support coordinated risk management, incident response and business continuity arrangements.

Security by Design

Security considerations shall be incorporated into the planning, design, refurbishment and management of University buildings, infrastructure and major projects at the earliest practicable stage.

The Head of Security shall be consulted on significant construction projects, refurbishments and changes in building use to ensure that appropriate protective security measures are considered alongside operational, health and safety, fire safety and accessibility requirements.

Security measures should be proportionate to the identified risks and seek to balance effective protection with the University's commitment to providing an open, inclusive and welcoming environment.

6.8 Security Systems

The University operates a range of electronic and physical security systems to support the protection of people, property, information and infrastructure across its campuses. These systems form an integral part of the University's wider security strategy and shall be managed in accordance with this policy and associated operational procedures.

Security systems are designed to support the prevention and detection of crime, enhance situational awareness, manage access to University premises and assist in responding to security incidents and emergencies.

The deployment, operation and maintenance of security systems shall be proportionate to identified risks and regularly reviewed to ensure they remain effective and appropriate.

Electronic Access Control

The University operates electronic access control systems to manage entry to buildings, rooms and other controlled areas. Access permissions shall be allocated according to operational need and the principle of least privilege. Electronic access permissions shall be reviewed periodically and amended promptly following changes to an individual's role, responsibilities or employment status.

Access control records may be used to support investigations into security incidents, safeguarding concerns, disciplinary matters or criminal investigations where there is a legitimate operational or legal requirement.

Closed Circuit Television (CCTV)

The University operates CCTV systems across its estate in accordance with the University's Closed Circuit Television (CCTV) Policy.

CCTV supports the prevention and detection of crime, the investigation of incidents, safeguarding, the protection of University assets and the safety of staff, students and visitors. The operation, management, disclosure and retention of CCTV images are governed by the University's CCTV Policy and associated operational procedures.

Intruder Detection Systems

Intruder alarm systems are installed within designated buildings and areas where appropriate to support the protection of University premises and assets. Alarm activations shall be investigated by the Security Team or an authorised monitoring provider in accordance with established response procedures.

Unauthorised interference with intruder alarm systems is prohibited and may result in disciplinary action.

Security Communications

The University maintains appropriate communication systems to support the coordination of security operations and emergency response.

These may include:

- Security radios;
- Emergency telephones;
- Help points;
- Alarm monitoring systems;
- Mass notification systems;
- Safe Zone;
- Other approved communication technologies

Security-critical communication systems shall be maintained to ensure resilience and availability during normal operations and emergency situations.

Security System Management

The Head of Security is responsible for ensuring that security systems remain operationally effective and continue to support the University's security objectives.

Changes to security systems shall be subject to appropriate planning, testing and approval before implementation. Where significant changes are proposed, the Head of Security shall be consulted during the planning stage to ensure that security requirements are fully considered.

Security systems shall be maintained by competent persons in accordance with manufacturer recommendations, contractual arrangements and relevant British Standards. Routine testing, preventative maintenance and periodic inspections shall be undertaken to verify system performance and identify faults requiring corrective action.

System Resilience

The University shall seek to ensure that critical security systems remain resilient and capable of supporting security operations during foreseeable incidents. Business continuity arrangements shall be maintained to minimise disruption following equipment failure, power outages, cyber incidents or other events affecting security infrastructure.

Where a security system becomes unavailable, appropriate interim measures shall be implemented until normal service is restored. The Security Team shall maintain procedures for responding to significant failures affecting security systems and shall notify relevant stakeholders where operational impacts are identified.

Security Technology Governance

The procurement, design, installation and replacement of security technologies shall be undertaken in consultation with the Head of Security to ensure systems remain interoperable, proportionate and aligned with the University's security strategy.

New security technologies shall, where reasonably practicable, comply with recognised industry standards and be capable of integration with existing security infrastructure.

Cyber-Physical Security

Where security systems rely upon network connectivity or digital infrastructure, they shall be implemented and managed in partnership with Information Technology Services to ensure appropriate cyber security controls, resilience and system availability are maintained throughout their operational lifecycle.

6.9 Counter Terrorism and Protective Security

City St George's, University of London recognises that higher education institutions may be attractive targets for terrorism and other hostile acts because of their open environments, diverse communities, internationally recognised research, public accessibility and critical infrastructure.

The University is committed to adopting a proportionate, intelligence-led and risk-based approach to protective security that balances the need to provide an open and welcoming environment with the responsibility to protect people, property and University operations.

Protective security arrangements shall be developed, implemented and reviewed in accordance with current threat assessments, legislative requirements and recognised good practice.

Protective Security

The University shall implement protective security measures that are proportionate to the identified risks affecting its campuses, buildings, events and activities.

Protective security measures may include:

- Physical security measures;
- Electronic security systems;
- Access control arrangements;
- Hostile vehicle mitigation where appropriate;
- Visitor management procedures;
- Security screening where justified;
- Protective landscaping and environmental design;
- Security awareness initiatives;
- Emergency planning arrangements.

Protective security measures shall be reviewed periodically and whenever significant changes occur to the University's operations, estate, threat environment or legislative requirements.

Terrorism Preparedness

The University shall maintain arrangements to prepare for, respond to and recover from incidents involving terrorism or other hostile acts.

These arrangements shall include:

- Security risk assessments;
- Protective security planning;
- Incident response plans;
- Evacuation and invacuation procedures;
- Lockdown arrangements where appropriate;
- Business continuity arrangements;
- Recovery planning;
- Multi-agency liaison.

The University shall maintain effective relationships with the Police Counter Terrorism Security Advisors (CTSAs), emergency services, local resilience partners and other relevant agencies.

Terrorism (Protection of Premises) Act 2025 (Martyn's Law)

The University is committed to meeting its obligations under the Terrorism (Protection of Premises) Act 2025 and associated statutory guidance.

Where applicable, the University shall:

- Assess the vulnerability of relevant premises and activities;
- Implement reasonably practicable public protection procedures;
- Maintain appropriate security plans;
- Provide relevant training and awareness to staff;
- Ensure appropriate governance and oversight arrangements are in place;
- Periodically review preparedness arrangements.

Compliance with statutory duties shall be monitored through the University's governance framework.

Security Awareness

The University recognises that informed and vigilant staff and students are among its most effective security measures.

The University shall promote security awareness through appropriate communications, training and engagement activities. Where appropriate, staff whose roles involve security responsibilities shall receive training relevant to their duties.

The University supports nationally recognised security awareness initiatives including:

- ACT (Action Counters Terrorism) Awareness;
- ProtectUK guidance;
- Run, Hide, Tell;
- CitizenAID;
- other protective security guidance issued by the National Protective Security Authority (NPSA), Home Office or Counter Terrorism Policing.

Events

Security arrangements for University events shall be proportionate to the nature, size and risk profile of the activity. Where appropriate, event organisers shall undertake security risk assessments in consultation with the Head of Security.

Additional protective security measures may be implemented for events involving:

- Large audiences;
- High-profile speakers;
- Controversial topics;
- Visiting dignitaries;
- Increased public attendance;
- Elevated threat assessments.
- Reporting Suspicious Activity

All members of the University community are expected to remain vigilant and report suspicious behaviour, suspicious items or security concerns immediately.

Examples include:

- suspicious packages;
- hostile reconnaissance;
- unauthorised attempts to access restricted areas;
- unattended vehicles in unusual locations;
- behaviour causing concern for public safety.

Reports should be made immediately to the Security Team or, where there is an immediate threat to life, directly to the emergency services.

Protective Security by Design

Security considerations shall be incorporated into the planning, design, refurbishment and management of University buildings, public spaces and major projects.

The Head of Security shall be consulted during the planning and design stages of significant developments to ensure that protective security measures are considered alongside operational, health and safety, fire safety, accessibility and sustainability requirements.

Where appropriate, recognised design principles, including Crime Prevention Through Environmental Design (CPTED) and guidance issued by the National Protective Security Authority (NPSA), shall be considered during the design and delivery of projects.

Continuous Improvement

The University's protective security arrangements shall be reviewed periodically to reflect:

- Changes in the national threat level;
- Intelligence received from policing or government agencies;
- Legislative developments;
- Lessons identified following incidents or exercises;
- Changes to the University's estate or operational activities.

The Head of Security shall provide strategic advice to the University Executive regarding emerging threats, protective security priorities and recommendations for continuous improvement.

The University shall seek continual improvement in protective security maturity through the adoption of recognised sector good practice, independent assurance, peer review and engagement with organisations including AUCSO, ProtectUK, the National Protective Security Authority and Counter Terrorism Policing.

6.10 Personal Safety and Lone Working

The University is committed to providing a safe and secure environment in which staff, students, contractors and visitors can work, study and undertake University activities. Whilst the University will implement appropriate security measures, all members of the University community are expected to take reasonable responsibility for their own personal safety and to remain aware of their surroundings.

Personal safety should be considered as part of routine working practices, particularly where activities are undertaken outside normal operating hours, in isolated locations or where there is an increased risk of confrontation or violence.

Personal Safety

Individuals are encouraged to:

- Remain vigilant and aware of their surroundings;
- Avoid placing themselves in situations that present an unnecessary risk;
- Report suspicious behaviour, hazards or security concerns promptly;
- Challenge unknown individuals where it is safe and appropriate to do so, or report concerns to the Security Team;
- Safeguard personal belongings and University property;
- Comply with local security procedures and emergency instructions.

Where an individual believes that their safety, or the safety of others, is at immediate risk, they should contact the Security Team or, where appropriate, the emergency services without delay.

Lone Working

The University recognises that some staff may be required to work alone as part of their normal duties or outside normal operating hours. Lone working shall only be undertaken where appropriate risk assessments have been completed and suitable control measures are in place.

Managers are responsible for ensuring that lone working arrangements within their areas are regularly reviewed and remain appropriate to the risks involved.

Control measures may include:

- Agreed communication arrangements;
- Scheduled welfare checks;
- Personal safety devices;
- Safe Zone App
- Access to emergency communications;
- Restrictions on higher-risk activities;
- Local supervision arrangements.

Lone workers shall ensure that they are familiar with local emergency procedures and know how to obtain assistance should it become necessary.

Violence, Aggression and Conflict

The University operates a zero-tolerance approach towards violence, aggression, intimidation, harassment or threatening behaviour directed towards members of the University community.

Where staff are confronted by aggressive or threatening behaviour they should, wherever practicable:

- Prioritise their own personal safety;
- Attempt to de-escalate the situation where it is safe and appropriate to do so;
- Withdraw from the situation where necessary;
- Request assistance from the Security Team or emergency services;
- Report the incident in accordance with University procedures.

Security personnel shall respond to reports of violence or aggression in accordance with their operational procedures and training.

Welfare Support

The University recognises that security incidents may have a significant impact upon the wellbeing of those involved.

Following serious incidents, appropriate welfare support shall be made available through the University's established support services, which may include Occupational Health, Human Resources, Student Support Services or other appropriate providers. Managers should ensure that appropriate welfare considerations form part of the post-incident response and recovery process.

Personal Security During Emergencies

During emergencies or major incidents, individuals shall follow instructions issued by the Security Team, emergency services or other authorised persons. Where evacuation, invacuation or lockdown procedures are implemented, all persons on University premises are expected to comply promptly with instructions issued for their safety.

Following any significant incident, the University shall review the effectiveness of its response and identify opportunities to strengthen personal safety arrangements through continuous improvement.

Emergency Procedures

Individuals should familiarise themselves with the University's emergency procedures, including evacuation, invacuation and lockdown arrangements, and participate in training or exercises where required.

6.11 Standards of Behaviour and Security Compliance

The University is committed to maintaining a safe, secure, respectful and inclusive environment for all members of the University community. All staff, students, contractors and visitors are expected to conduct themselves in a manner that supports the safety, wellbeing and security of others whilst using University premises or participating in University activities.

Individuals shall comply with all reasonable instructions issued by Security personnel, authorised University staff or emergency responders where those instructions relate to safety, security or the effective management of an incident. Failure to comply with reasonable instructions may result in removal from University premises, withdrawal of access privileges or other action in accordance with University regulations and procedures.

Unacceptable Behaviour

Behaviour that compromises the safety, security or wellbeing of others will not be tolerated.

Examples of unacceptable behaviour include, but are not limited to:

- Violence or threats of violence;
- Abusive, aggressive or intimidating behaviour;
- Harassment, discrimination or victimisation;
- Deliberate damage to University property;
- Theft, fraud or other criminal activity;
- Unauthorised access to buildings or restricted areas;
- Misuse of University identification cards, keys or access credentials;
- Interference with security systems or safety equipment;
- Failure to comply with evacuation, lockdown or other emergency procedures;
- Possession of offensive weapons without lawful authority;
- Behaviour that places others at unnecessary risk.

The examples above are not exhaustive and the University reserves the right to take appropriate action where behaviour is considered incompatible with maintaining a safe and secure environment.

Alcohol and Drugs

Individuals attending University premises shall not be under the influence of alcohol or drugs where doing so creates a risk to their own safety or the safety of others. The possession, use, supply or production of controlled drugs or psychoactive substances on University premises is prohibited unless lawfully prescribed or otherwise authorised.

Where alcohol is served as part of an authorised University event, organisers shall ensure that appropriate management arrangements are implemented to minimise foreseeable risks.

Where Security personnel reasonably believe that an individual's behaviour presents an immediate risk due to intoxication or substance misuse, appropriate action may be taken to safeguard those involved, including requesting assistance from the emergency services where necessary.

Offensive Weapons

The possession of firearms, imitation firearms, offensive weapons or other items intended for use as weapons on University premises is prohibited except where expressly authorised by the University or where required by emergency services or other statutory agencies acting in the course of their duties.

Any person found in possession of an offensive weapon, or suspected of carrying such an item, shall be reported immediately to the Security Team. Security personnel shall manage such incidents in accordance with the University's emergency procedures and, where appropriate, notify the Police without delay.

Compliance with Security Procedures

Members of the University community shall comply with published security procedures relating to:

- Access control;
- Identification cards;
- Visitor management;
- Reporting security incidents;
- Emergency response;
- Protective security measures;
- Safeguarding University property.

Individuals shall cooperate with reasonable security checks where these are necessary to protect the safety of people, property or University operations.

Authorised Security personnel may request proof of identity or authority to remain on University premises where there are reasonable grounds to do so in the interests of safety, security or the prevention and detection of crime.

Removal from University Premises

The University reserves the right to refuse entry to, or require the removal of, any individual whose behaviour presents a risk to the safety, security or wellbeing of others or who fails to comply with this policy or reasonable instructions issued by authorised personnel. Where appropriate, such action may be taken in conjunction with disciplinary procedures, student conduct procedures, contractual remedies or criminal investigation.

Reporting and Investigation

Security incidents involving unacceptable behaviour shall be reported promptly and recorded in the University's incident management system. Where appropriate, incidents shall be investigated by the Security Team in collaboration with Human Resources, Student & Academic Services, departmental management or external agencies.

Evidence gathered during investigations, including CCTV footage, access control records, witness statements and other relevant information, shall be managed in accordance with University procedures and applicable legislation.

Lessons identified following incidents shall be used to strengthen security arrangements, improve awareness and inform future policy development.

6.12 Lost and Found Property

City St George's, University of London is committed to supporting the return of lost property to its rightful owner wherever reasonably practicable. The University shall maintain appropriate arrangements for the receipt, recording, storage, return and disposal of lost property found on University premises.

The Security Team shall normally act as the central point for the management of lost property unless alternative local arrangements have been approved for specific areas or campuses.

Reporting Lost Property

Any person who loses personal property whilst on University premises is encouraged to report the loss to the Security Team as soon as reasonably practicable.

Where possible, reports should include:

- A description of the item;
- The location where it was last seen;
- The date and approximate time it was lost;
- Any identifying features that may assist with identification.

The University will make reasonable efforts to assist in locating lost property but cannot guarantee its recovery.

Property Found on University Premises

Any member of the University community who finds property on University premises shall hand the item to the Security Team, University Reception or other authorised collection point at the earliest opportunity. Items shall not be retained for personal use or removed from University premises unless authorised for the purposes of returning them to their rightful owner.

The Security Team shall maintain appropriate records of all property received, including:

- A description of the item;
- The date and location where it was found;
- The individual who handed the item in, where known;
- The action taken;
- The date the item was returned or otherwise disposed of.
- Storage and Security

Lost property shall be stored securely in a designated location with access restricted to authorised personnel. Additional security arrangements shall be implemented for items of significant financial value, confidential information, controlled items or property that may present a safety or security risk.

Perishable items may be disposed of without delay where retention would present a health risk.

Return of Property

Where ownership can be reasonably established, the University shall make reasonable efforts to contact the owner and arrange for the return of the property.

Individuals collecting property may be required to:

- Provide satisfactory proof of identity;
- Provide sufficient information to demonstrate ownership;
- Sign to acknowledge receipt of the item.

The University reserves the right to refuse the release of property where ownership cannot be satisfactorily established.

Disposal of Unclaimed Property

Property that remains unclaimed after a reasonable retention period may be disposed of in accordance with the University's approved procedures.

Depending upon the nature of the item, disposal may include:

- Recycling;
- Donation to charity;
- Secure destruction;
- Disposal as waste;
- Transfer to the Police or other statutory authority where appropriate.

Items containing personal data shall be disposed of securely in accordance with the University's Data Protection Policy and Records Management Policy.

High Value, Dangerous or Illegal Items

Items of significant financial value, suspected stolen property, controlled drugs, offensive weapons, firearms, hazardous substances or any item believed to be connected with criminal activity shall be reported immediately to the Security Team. Such items shall not normally be returned directly to an individual without appropriate authorisation and, where necessary, consultation with the Police or other relevant authority.

The University reserves the right to retain such items where required to support a criminal investigation or other lawful purpose.

Liability

The University accepts no responsibility for the loss of personal property brought onto University premises except where liability arises through the negligence of the University. Members of the University community remain responsible for taking reasonable care of their personal belongings at all times.

The existence of a lost property process does not remove an individual's responsibility to safeguard their own possessions.

6.13 Vehicles, Motorcycles and Cycles

The University is committed to maintaining a safe, secure and accessible environment for all users of its campuses. Appropriate arrangements shall be implemented to manage vehicles, motorcycles and cycles on University premises in a manner that supports safety, security and the effective operation of the estate.

The management of parking and traffic shall balance operational requirements with the need to protect pedestrians, maintain emergency access and safeguard University property.

Access to University Premises

Vehicle access to University premises shall be managed in accordance with local campus arrangements and operational requirements. Access to designated service roads, restricted parking areas, loading bays and controlled vehicle access points may be limited to authorised vehicles or individuals with prior approval.

Security personnel may request proof of authority to access restricted vehicle areas where necessary to protect the safety and security of the University community. The University reserves the right to refuse or withdraw vehicle access where there are reasonable grounds to do so in the interests of safety, security or operational necessity.

Parking

Vehicles shall be parked only within designated parking areas and in accordance with University parking arrangements.

Vehicles shall not be parked in locations that:

- Obstruct emergency access routes.
- Restrict pedestrian movement.
- Prevent access to buildings or facilities.
- Obstruct fire exits, emergency equipment or service areas.
- Create a safety or security risk.

The University may take appropriate action where vehicles are parked in an unsafe or unauthorised manner, including restricting future access or requesting removal.

Motorcycles and Cycles

The University supports sustainable travel and encourages the use of motorcycles and cycles where appropriate.

Motorcycles and cycles should be secured using suitable security devices and, where available, parked within designated parking or storage facilities. The University encourages the use of appropriate security measures, including approved locks and other theft prevention devices, to reduce the risk of theft.

Motorcycles and cycles shall not be stored within buildings, stairwells, corridors, emergency escape routes or any location that may create an obstruction or compromise fire safety unless specifically authorised.

Security of Vehicles

Owners and users of vehicles are responsible for taking reasonable precautions to protect their vehicles and any property contained within them.

Individuals should:

- Ensure vehicles are locked and secured when unattended.
- Remove valuables from sight wherever practicable.
- Avoid leaving University equipment or confidential information unattended within vehicles.

- Report suspicious activity, attempted theft or criminal damage to the Security Team immediately.

The University may operate CCTV and other security measures within vehicle parking areas in accordance with the University's CCTV Policy.

Electric Vehicles and Charging Facilities

Where electric vehicle charging facilities are provided, they shall be used only for their intended purpose and in accordance with the University's published guidance. Charging equipment shall not be tampered with or used in a manner that may present a safety or security risk.

The installation of personal charging equipment on University premises is prohibited unless expressly authorised by the University.

Abandoned, Dangerous or Unauthorised Vehicles

Vehicles that appear to be abandoned, insecure, causing an obstruction or presenting a safety or security concern may be investigated by the Security Team.

Where appropriate, the University may:

- Attempt to identify and contact the registered user.
- Restrict access to affected areas.
- Request the removal of the vehicle.
- Notify the Police, Local Authority or other relevant agency.
- Implement temporary protective measures where necessary.

Vehicles giving rise to security concerns, including those suspected of being associated with criminal activity or presenting a potential threat to public safety, shall be managed in accordance with the University's emergency procedures.

Liability

Vehicles, motorcycles, cycles and their contents remain the responsibility of their owners at all times.

The University accepts no responsibility for loss of, or damage to, vehicles or their contents unless liability arises through the negligence of the University. The provision of parking facilities or cycle storage does not imply acceptance of responsibility for the security of vehicles or personal property left on University premises.

6.14 Operational Assurance, Review and Continuous Improvement

The University is committed to maintaining effective, resilient and proportionate security arrangements through the regular review of operational performance, emerging risks and lessons identified from incidents, exercises and stakeholder feedback.

Operational assurance activities shall support the continual improvement of the University's security arrangements and ensure that security measures remain aligned with organisational objectives, legislative requirements and recognised good practice.

Operational Monitoring

The Head of Security shall establish appropriate arrangements to monitor the effectiveness of operational security measures across the University.

Monitoring activities may include:

- Reviewing Security Incident Reports and emerging trends.
- Analysing response times and operational performance.
- Monitoring crime patterns affecting the University community.
- Reviewing access control activity and associated audit records.
- Monitoring the performance and availability of security systems.
- Assessing compliance with security procedures and local operating arrangements.
- Reviewing feedback received from staff, students, visitors and partner organisations.

Operational information shall be used to identify opportunities to improve security arrangements and reduce organisational risk.

Security Risk Reviews

Security risks shall be reviewed regularly to ensure that protective measures remain appropriate and proportionate.

Reviews shall be undertaken:

- Following significant security incidents.
- Following changes to the University's estate, operations or activities.
- Where intelligence indicates changes in the threat environment.
- Following changes in legislation or recognised good practice.
- As part of planned security assurance activities.

Where necessary, additional control measures shall be introduced to address identified risks.

Exercises and Debriefs

The University shall periodically test its security and emergency arrangements through exercises, simulations, desktop activities and other assurance activities where appropriate.

Following exercises or significant incidents, structured debriefs shall be undertaken to identify:

- Good Practice that should be retained.
- Areas for Improvement.
- Lessons Identified.
- Actions Required to strengthen future preparedness.

Improvement actions shall be allocated to appropriate individuals and monitored until completion.

Performance Reporting

The Head of Security shall provide periodic reports to the Assistant Director – Facilities Management and other appropriate governance groups regarding the effectiveness of the University's security arrangements.

Reports may include information relating to:

- Security Performance Indicators.
- Incident Trends.

- Protective Security Initiatives.
- Counter Terrorism Preparedness.
- Security Risks.
- Compliance Activities.
- Progress against agreed security improvement plans.

Where significant issues are identified, these shall be escalated through the University's governance arrangements.

Continuous Improvement

The University is committed to fostering a culture of continual improvement in the management of physical security. Security policies, procedures and operational practices shall be reviewed regularly to ensure that they remain effective, proportionate and responsive to changing risks.

The University shall seek continual improvement through:

- Implementing recommendations arising from incidents, audits and inspections.
- Engaging with recognised sector guidance and best practice.
- Collaborating with emergency services, partner organisations and professional networks.
- Investing in appropriate training, technology and security capability.
- Reviewing emerging threats and opportunities to strengthen protective security.
- Promoting a positive security culture across the University community.

The University recognises that effective security depends not only upon physical measures and technology, but also upon informed decision-making, strong governance and the active participation of the entire University community. Continuous improvement shall therefore remain a fundamental principle underpinning all aspects of the University's security arrangements.

7 Advice and Guidance

The University recognises that effective security relies upon clear communication, appropriate guidance and access to competent advice.

Members of the University community are encouraged to seek advice where they are uncertain about the application of this policy, the operation of security procedures or the management of security risks.

Advice should be sought before undertaking activities that may have implications for the safety and security of individuals, University property or University operations.

7.1 Security Advice

Advice relating to the interpretation of this policy, physical security measures, access control, security systems, incident reporting, crime prevention or protective security should be obtained from the Head of Security or an authorised member of the Security Management Team.

The Security Team will provide advice proportionate to the nature of the request and may liaise with other University departments or external agencies where specialist expertise is required.

7.2 Risk Management and Protective Security

Advice relating to security risk assessments, protective security measures, major events, hostile vehicle mitigation, security by design or counter terrorism preparedness should be sought through the Head of Security.

Where appropriate, the University may consult with external partners, including the Police, Counter Terrorism Security Advisers (CTSAs), the National Protective Security Authority (NPSA), ProtectUK or other competent authorities to ensure that security arrangements reflect current good practice.

7.3 Related Policies and Procedures

This policy should be read in conjunction with other relevant University policies, procedures and guidance, including but not limited to:

- Health and Safety Policy.
- Fire Safety Policy.
- Closed Circuit Television (CCTV) Policy.
- Information Security Policy.
- Data Protection Policy.
- Visitor Management Policy.
- Emergency Management Plan.
- Business Continuity Framework.
- Relevant Local Security Procedures.

Where there is any uncertainty regarding the relationship between this policy and another University policy or procedure, advice should be sought from the Head of Security or the relevant policy owner.

7.4 Training and Awareness

The University will provide appropriate security training, information and awareness activities to support the implementation of this policy.

Training requirements will vary according to an individual's role and responsibilities and may include:

- General Security Awareness.
- Incident Reporting Procedures.
- Emergency Response Arrangements.
- Protective Security Awareness.
- Counter Terrorism Awareness.
- Conflict Management.
- Use of Security Systems.
- Role-Specific Operational Training.

Staff are expected to complete mandatory security training where it forms part of their role or where required by University procedures.

Managers shall support staff in maintaining appropriate levels of security awareness and competence relevant to their responsibilities.

8 Failure to comply

Compliance with this policy is essential to maintaining a safe, secure and resilient environment across City St George's, University of London. All members of the University community are expected to comply with the requirements of this policy, associated procedures and any reasonable instructions issued by authorised University personnel in relation to security matters.

Failure to comply with this policy may compromise the safety of individuals, the security of University property, the continuity of University operations and the University's ability to meet its statutory and regulatory obligations.

Where non-compliance is identified, the University will consider the nature, seriousness and circumstances of the breach before determining an appropriate course of action.

Failure to comply with this policy may result in one or more of the following:

- Informal Advice or Corrective Action where appropriate.
- Withdrawal or Restriction of access to University buildings, systems or facilities.
- Mandatory Retraining or additional security awareness requirements.
- Investigation under the University's disciplinary, capability or student conduct procedures, where applicable.
- Termination of contracts, agreements or access arrangements for contractors, consultants or third parties.
- Referral to external agencies, including the Police or regulatory authorities, where criminal offences or statutory breaches are suspected.
- Civil Recovery or Legal Action where appropriate to protect the University's interests.

Nothing within this policy prevents the University from taking immediate action where this is necessary to protect life, maintain public safety, safeguard University property or prevent further harm. The University will ensure that any action taken in response to non-compliance is fair, proportionate and consistent with the University's policies, procedures and legal obligations.

Any concerns regarding the application of this policy or allegations of non-compliance should be reported through the appropriate management or Security reporting arrangements to ensure they are investigated and addressed appropriately.

9 Policy Review and Document Control

This policy shall be reviewed at least every three years, or sooner where necessary to ensure that it remains effective, compliant with legislation and aligned with the University's strategic objectives.

An earlier review may be undertaken where there are significant changes to:

- Legislation, statutory guidance or regulatory requirements.
- The University's Organisational Structure or governance arrangements.
- The University's Estate, operational activities or risk profile.
- The National Security Threat Environment.
- Relevant British Standards, Government guidance or recognised sector good practice.
- Security Technologies or operational practices.
- Recommendations arising from incidents, audits, inspections or exercises.

The Head of Security is responsible for reviewing this policy and recommending amendments where appropriate.

Any proposed amendments shall be subject to the University's policy governance and approval processes before implementation. Minor administrative amendments, including corrections to job titles, organisational names, contact details, references, hyperlinks or formatting, may be approved through the University's document control arrangements where they do not materially alter the intent or operation of the policy.

The review process shall include consultation with relevant stakeholders to ensure that the policy remains practical, proportionate and reflective of the University's operational requirements.

Superseded versions of this policy shall be retained and managed in accordance with the University's Records Management Policy and document retention requirements.

Responsibility for implementing this policy rests with all members of the University community; however, overall responsibility for maintaining and reviewing the policy rests with the Head of Security, under the strategic oversight of the Assistant Director – Facilities Management.

Policy information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact Chris Saich, Head of Security.

Policy Title:	City St Georges Security Policy
Policy Version:	V1.0
Primary Author:	Chris Saich, Head of Security
Related Policies:	Closed Circuit Television (CCTV) Policy Data Protection Policy Emergency Management Plan Fire Safety Policy Health and Safety Policy Information Security Policy IT Acceptable Use Policy Lone Working Policy Safeguarding Policy Visitor Management Policy
Accountable Authority:	Velda Ismay. Assistant Director Facilities Management
Approving Authority:	University Health and Safety Committee
Date of Approval:	TBC
Policy effective from:	TBC
Date of Review:	One year from approval date

