Name of policy – Information Security Policy

Version number – v1.0

Effective date - 29 April 2026

INFORMATION SECURITY POLICY
v1.0

Policies superseded by this version

This document replaces the Legacy Information Security Policy (ITPOL01) of City, University of London, and the legacy information security arrangements of St George's University of London, with effect from [*date*].

Summary of changes to previous version

This policy has been *re-written* following a review due to the merger of City University of London and St George's University of London.

Table of contents

1 Introduction

City St George's, University of London ("the University") processes information to carry out its core functions in teaching, research and administration. This may include confidential, commercially sensitive and personal information about individuals and organisations. Information is a valuable asset. The continuity of University operations and the progress of academic work depend on its integrity and availability.

This policy is the overarching information security policy for the University. It establishes the University's commitment to protecting information assets from unauthorised access, use, modification, disclosure or destruction, whether accidental or intentional. It provides the authority and governance framework for the University's Information Security Management System (ISMS), which is aligned to ISO/IEC 27001:2022.

All subsidiary information security policies, standards and procedures derive their authority from this policy. This policy, and the ISMS it governs, supports the University's compliance with applicable legal, regulatory and contractual obligations including the UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, the Prevent duty and sector-specific requirements.

1.1 Freedom of Speech and Academic Freedom

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.

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.

1.2 Equity, Diversity and Inclusion

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.

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.

2 Definitions

For the purpose of this document, the terms and definitions given in ISO/IEC 27001:2022 apply. Standard IT terminology is used throughout.

1. Information asset – Any data, system, service or infrastructure component that has value to the University.

2. Information security – The preservation of the confidentiality, integrity and availability of information.

3. ISMS – Information Security Management System – the framework of policies, procedures, controls and risk management processes designed to protect information assets, aligned to ISO/IEC 27001:2022.

4. Confidentiality – Ensuring that information is accessible only to those authorised to access it.

5. Integrity – Safeguarding the accuracy and completeness of information and processing methods.

6. Availability – Ensuring that authorised users have access to information and associated assets when required.

7. Risk owner – The person or entity with the accountability and authority to manage a risk.

8. Subsidiary policy – A policy that forms part of the ISMS and derives its authority from this Information Security Policy.

3 Scope

This policy applies to all staff, students, researchers, visiting academics, contractors, consultants, agency workers, volunteers, honorary staff, alumni with active accounts and any third parties authorised to access University information or systems.

This policy covers all information assets owned, managed or processed by the University, or processed on its behalf, in whatever form. This includes electronic data, paper records, verbal communications and information held by third-party service providers acting on the University's behalf.

This policy applies to all information processing activities, whether conducted on university premises or remotely, using University-owned or other equipment, and regardless of the technology platform or medium used.

This policy is reviewed, maintained and updated by the Information Security Manager. It will be reviewed at minimum annually or following significant change.

4 Policy

The University is committed to protecting and securing the use of information and information systems under its control to maintain the confidentiality, integrity and availability of its information assets.

4.1 Information security purpose and commitments

The University shall:

- Maintain an Information Security Management System (ISMS) aligned to ISO/IEC 27001:2022, supported by appropriate policies, procedures and technical controls.
- Use a risk-based approach when assessing the risks associated with information assets, applying physical, personnel, technical and procedural measures to achieve appropriate and proportionate security.
- Consider developments in technology, the threat landscape and the costs of implementation in order to achieve a level of security appropriate to the nature and value of the information being protected and the harm that could result from a security breach.
- Provide staff, students and other users with access to information, which may include personal data, only where it is required to perform their role or fulfil authorised requirements, on the basis of least privilege.
- Provide information security awareness, education and training to staff, students and other users to enable them to understand and carry out their responsibilities.
- Monitor compliance with security obligations and take appropriate action where non-compliance is identified.
- Use ISO/IEC 27001:2022, Cyber Essentials Plus, the NIST Cybersecurity Framework and associated standards as the basis for its information security governance.
- Comply with all applicable legislative and regulatory requirements, including the UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, the Regulation of Investigatory Powers Act 2000, the Terrorism Act 2006 and the Higher Education (Freedom of Speech) Act 2023.
- Establish and maintain appropriate relationships with law enforcement authorities, regulatory bodies, sector organisations and network and telecommunications operators in support of its information security objectives.
- Pursue continual improvement of the ISMS through management review, internal audit, incident analysis and the correction of non-conformities.

4.2 ISMS framework

The University's ISMS comprises a suite of subsidiary policies, standards, procedures and guidelines that together provide the detailed controls and operational requirements for information security. All subsidiary policies derive their authority from this policy and must be read in conjunction with it.

The ISMS is structured across the following domains: governance and risk management, access control and identity management, data protection and classification, network and infrastructure security, incident management and business continuity, third-party and supply chain security, and monitoring, audit and compliance.

Subsidiary policies are approved via the Information Governance and Security Committee (IGSC) and maintained by the Information Security Manager. A register of all ISMS policies and their review dates is maintained and published on the University intranet.

4.3 Information classification and handling

Information assets will be handled with a level of protection appropriate to their sensitivity and value. The University will develop and maintain guidance on the handling and storage of information based on its sensitivity, in line with ISO/IEC 27001:2022 Annex A control A.5.12."

4.4 Risk management

The University shall adopt a systematic approach to information security risk management, consistent with ISO/IEC 27001:2022 Clauses 6 and 8. Risks to information assets will be identified, assessed, treated and monitored on a regular basis.

Risk assessments will be conducted for new systems, services and significant changes to existing systems. Risk treatment decisions will be documented and approved by the appropriate risk owner. Residual risks that exceed the University's risk appetite must be escalated to the Chief Information Officer or the IGSC for acceptance.

IGSC will maintain an information security risk register, which will be reviewed at least quarterly. Information security risks of institutional significance will be escalated to the University's central risk register.

4.5 Incident management

All actual or suspected information security incidents must be reported immediately to the IT Service Desk or through the University's incident-reporting channels. Incidents will be logged, assessed, contained and resolved in accordance with the University's Information Security Incident Management Policy.

Where an incident involves personal data, the Data Protection Officer must be notified without delay to assess whether notification to the Information Commissioner's Office or affected individuals is required under the UK GDPR.

4.6 Business continuity

Information security controls will be integrated into the University's business continuity and disaster recovery arrangements. Critical information systems and data will be identified, and appropriate resilience, backup and recovery measures will be maintained to support the continuity of university operations.

5 Roles and responsibilities

Effective information security relies on all users understanding and fulfilling their responsibilities. The following roles have specific duties in relation to this policy and the ISMS:

a. Senior Information Risk Owner (SIRO)

The Deputy President (Operations) acts as the SIRO and owns the overall information risk for the University. The SIRO chairs the Information Governance and Security Committee (IGSC) and is accountable for ensuring that information risks are managed effectively across the institution.

b. Chief Information Officer (CIO) and Deputy CIO

The CIO holds operational accountability for information security, supported by the Deputy CIO. Together they ensure that appropriate technical, procedural and governance measures are in place to support the ISMS, approve security exceptions and escalate risks that exceed the University's risk appetite.

c. Information Security Manager

Maintains this policy and the ISMS, oversees the implementation of information security controls, provides expert advice, conducts risk assessments, manages the security incident response process and monitors compliance through audits, reviews and security assurance activities.

d. Data Protection Officer (DPO)

Advises on compliance with the UK GDPR and Data Protection Act 2018, assesses data protection risks, manages information rights requests and ensures that data protection considerations are integrated into information security controls and incident management.

e. Information Governance and Security Committee (IGSC)

Provides oversight, challenge and assurance for information security and governance matters, including policy approval, risk management and monitoring of compliance across the institution. The IGSC reports to the Senior Leadership Team and the Audit and Risk Committee.

f. Information Assurance Team

Responsible for advising on compliance with data protection legislation, managing the DPIA process, maintaining Records of Processing Activities and ensuring that organisational, procedural and technical controls collectively support a compliant and risk-aware environment.

g. Line managers and supervisors

Ensure that users within their teams understand and comply with information security policies, complete mandatory training and follow established procedures. Managers must notify IT promptly when staff or contractors change roles or leave the University.

h. System owners and data owners

Ensure that systems and information under their stewardship are classified correctly, protected in accordance with University standards and supported by appropriate risk assessments, DPIAs and access controls.

i. All users

All users are responsible for information security and must ensure that University systems are used in a secure and compliant manner. Users must protect their credentials, follow security guidance, complete mandatory training and report actual or suspected incidents without delay. For clarity, reporting obligations relate to specific security risks, policy breaches or unlawful activity, not the mere fact that opinions expressed may be controversial.

j. Third-party service providers

Where third parties process University data or provide technology services, they must comply with contractual requirements, applicable legislation and the University's security standards. Contract managers must ensure appropriate due diligence, risk assessments and data-processing agreements are in place.

6 Procedures

6.1 Compliance measurement

The Information Security Manager will verify compliance with this policy and subsidiary policies through periodic assessments, technical audits, penetration testing, business tool reports, internal and external audits and other assurance activities. Compliance reporting will be provided to the IGSC.

6.2 Security exceptions

Any exception to this policy or its subsidiary policies must be formally documented, risk-assessed and approved by the CIO or the IGSC. Exceptions will be time-limited and subject to periodic review. A register of active exceptions will be maintained by the Information Security Manager.

6.3 Third-party assurance

The University will conduct appropriate due diligence on third-party service providers who process University data or provide technology services. This includes assessing security posture, reviewing contractual terms and ensuring that data-processing agreements are in place where required.

6.4 Awareness and training

All users must complete mandatory information security awareness training and refresh it at intervals set by the University. Specialist training will be provided to users with elevated access or specific security responsibilities. The Information Security Manager will maintain records of training completion and report to the IGSC.

6.5 Policy maintenance

This policy and all subsidiary ISMS policies will be maintained in a central register. Each policy will have a designated owner, a defined review cycle and version control. Updates to subsidiary policies require approval by the IGSC.

7 Monitoring

Compliance with this policy and the ISMS will be monitored through a combination of technical controls, management review, internal audit and external assurance activities.

The University reserves the right to monitor and audit the use of its information systems in accordance with applicable legislation, including the Regulation of Investigatory Powers Act 2000 and the Lawful Business Practice Regulations 2000. Further detail is set out in the University's Monitoring, Logging and Audit Policy.

8 Advice and guidance

8.1 IT Service Desk

The first point of contact for general IT queries, technical support and reporting security incidents or concerns.

8.2 Information Security Manager

Provides specialist advice on information security controls, risk assessments, policy interpretation and compliance.

8.3 Data Protection Officer (DPO)

Offers guidance on UK GDPR and the Data Protection Act 2018, including data sharing, DPIAs, lawful basis for processing and information rights.

8.4 Information Assurance Team

Provides advice on data protection compliance, records management and information governance.

8.5 Additional guidance

Further information, technical standards and security guidance are available on the University intranet.

Users are encouraged to seek advice whenever they are uncertain about their obligations. Early engagement reduces risk and supports compliance.

9 Failure to comply

9.1 Users

Any reckless or wilful conduct by any person using the University's information systems which undermines this policy or puts at risk the security of information may result in withdrawal of access, mandatory retraining or other corrective measures. Serious or repeated breaches may lead to disciplinary action under the relevant University procedures for staff or students. Contractors and third-party users may have their access terminated and may be subject to contractual remedies.

9.2 Legal and regulatory obligations

Breaches involving personal data, security-sensitive materials, unauthorised access or other unlawful activity may be reported to external authorities where required, including law enforcement, the Information Commissioner's Office and any organisation whose systems or networks may have been affected.

9.3 Academic freedom and lawful expression

Actions taken under this policy will be applied consistently with the University's duties under the Higher Education (Freedom of Speech) Act 2023. Disciplinary or corrective measures will not be imposed for lawful academic expression or research activity.

10 Review

This policy shall be reviewed at least annually or following significant changes in legislation, technology, the threat landscape or organisational structure. Updates require approval by the Information Governance and Security Committee.

Risk management and continuous improvement

Risks related to information security will be recorded in the University risk register and reviewed at least quarterly. Findings from incidents, audits, management reviews and changes to the threat environment will feed into continual improvement of the ISMS in accordance with ISO/IEC 27001:2022 Clauses 9 and 10.

Policy information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact Information Security Manager, cybersecurity@citystgeorges.ac.uk.

Policy Title:	Information Security Policy
Policy Version:	Version 1.0
Primary Author:	Eric McIntosh
Related Policies:	
Accountable Authority:	IAT
Approving Authority:	IGSC
Date of Approval:	29 April 2026
Policy effective from:	29 April 2026
Date of Review:	

Appendix

Normative references

- ISO/IEC 27001:2022 Clauses 4–10 and Annex A controls A.5–A.8
- ISO/IEC 27002:2022 Controls 5–8
- NIST Cybersecurity Framework
- Cyber Essentials and Cyber Essentials Plus technical requirements
- UK GDPR and Data Protection Act 2018
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Lawful Business Practice Regulations 2000
- Human Rights Act 1998
- Terrorism Act 2006
- Higher Education (Freedom of Speech) Act 2023

All University IT security policies form the aligned ISMS suite governed by this Information Security Policy.