IT Acceptable Use Policy

version number v 92

[effective date] immediate

IT ACCEPTABLE USE POLICY
v92

Policies superseded by this version

This document replaces the Legacy Acceptable Use Policies of City University of London, and Legacy IT Conditions of Use Policy of St George's University of London, with effect from [*date*].

Summary of changes to previous version

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

Table of contents

1 Introduction

1.1 City St George's, University of London ("the University") is committed to maintaining the confidentiality, integrity and availability of its information assets. This policy defines acceptable behaviour and conditions of use for the University's information systems, ensuring compliance with legal, regulatory and contractual obligations and alignment with recognised security frameworks including ISO 27001:2022, NIST CSF, UK GDPR / DPA 2018 and Cyber Essentials.

All users share responsibility for protecting the University's information and technology resources, including hardware, software, data, network access, third-party services, online services and IT credentials.

This policy forms part of the University's Information Security Management System (ISMS), which is aligned to ISO/IEC 27001:2022.

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.

2.3 The Office for Students ("OfS") operates a free speech complaints scheme. Under that scheme, the OfS can review complaints about free speech from non-student members, staff, applicants for academic posts and (actual or invited) visiting speakers. The scheme is free to use. Information about the complaints that the OfS can review is available on its website at: www.officeforstudents.org.uk/for-providers/freedom-of-speech/free-speech-complaints. Student complaints about freedom of speech issues are handled by the Office of the Independent Adjudicator for Higher Education ("OIA"). Information about how the OIA handles such complaints can be found on its website (https://www.oiahe.org.uk/resources-and-publications/latest-news-and-updates/oia-highlights-role-in-student-free-speech-complaints/).

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

1. "The University" – City St George's, University of London.
2. Information asset – Data or system valuable to, operated or managed by the University.
3. User – Anyone granted access to University systems, including staff, students, contractors and third parties.
4. Personal data – Any information relating to an identified or identifiable living individual, as defined by the UK GDPR and DPA 2018.
5. Credentials – Usernames, passwords, passphrases, tokens, smart cards or any other identity mechanism used to authenticate access.
6. ISMS – The University's Information Security Management System, a systematic framework of policies, procedures, controls and risk management processes designed to protect the confidentiality, integrity and availability of information assets, aligned to ISO/IEC 27001:2022.
7. University network – All wired, wireless and virtual private network infrastructure operated by or on behalf of the University.
8. University-approved – Systems, services or tools that have been assessed, authorised and documented for use through appropriate University processes.

5 Policy

5.1 Purpose

The University is committed to ensuring that all use of its information systems is lawful, secure and responsible. This policy establishes the standards of behaviour expected of all users and provides the foundation for protecting University data, safeguarding users and maintaining the reliability and resilience of University technology services. The University expects all users to act with integrity, apply good judgement, respect the rights and freedoms of others and use information and systems only for legitimate academic, research or administrative purposes.

5.2 Scope

This policy applies to all users who access, use or interact with University information, systems, devices or network services. This includes staff, students, researchers, visiting academics, contractors, consultants, agency workers, volunteers, honorary staff, alumni with active accounts and any third parties authorised to use University resources.

The policy covers all information assets and technology resources owned, managed or provided by the University, or operated on its behalf. This includes University-owned laptops and desktops, mobile devices, servers, cloud services, storage platforms, networks, telephony, collaboration tools, specialist research systems and any personal devices used to access University services.

The policy applies to all use of University systems whether on campus or remote, using University-owned or personal equipment, and includes access via wired, wireless or virtual private networks.

Use of the University network is also subject to the JANET Acceptable Use Policy and other relevant external service terms, including Jisc and Eduroam regulations. When accessing services from another jurisdiction, users must abide by all relevant local laws as well as those applicable to the location of the service.

Compliance with this policy must be interpreted consistently with the University's legal obligations, including the UK GDPR, Data Protection Act 2018, Computer Misuse Act 1990, Higher Education (Freedom of Speech) Act 2023 and the Prevent duty. Nothing in this policy restricts lawful freedom of speech or academic freedom.

5.3 Principles

The University expects all users to uphold the following principles when accessing or using its information systems:

- Act lawfully, ethically and responsibly, ensuring that use of technology supports the University's academic mission and complies with all relevant legal and regulatory duties.
- Handle information in a manner that protects its confidentiality, integrity and availability.
- Access systems or data only as necessary for legitimate academic, research or administrative purposes.
- Respect the rights, dignity and lawful freedom of speech and academic freedom of others, recognising that robust or challenging academic discourse is permitted where it remains within the law.
- Safeguard information, follow security controls, report incidents promptly and contribute to a secure, resilient and trusted digital environment.

All users must:

- Take responsibility for protecting their credentials, including usernames and passwords, and never disclose them to any person. No member of staff has the authority to ask for a user's password.
- Enrol in and use multi-factor authentication (MFA) on all University systems and services. MFA is mandatory and must not be bypassed or disabled.
- Ensure that applications and systems are kept up to date on devices for which they are responsible and respond promptly to requests from IT to update or patch devices.
- Familiarise themselves with the University's information security, data protection and related policies and procedures.
- Report immediately if they detect, suspect or witness an actual or potential information security incident, through the IT Service Desk or the University's incident-reporting channels.
- Take reasonable precautions to protect all devices and media, including not leaving laptops or portable devices unattended or unsecured in public areas.

- Comply with the UK GDPR, DPA 2018 and any other legal, statutory or contractual obligations the University identifies as relevant.
- Only use University-approved storage systems to hold and store University data.
- Ensure that any work, research or project involving personally identifiable information has an appropriate Threshold Test or Data Protection Impact Assessment (DPIA) in place.
- Understand that use of the University network may be monitored in line with University policies and where there is a lawful basis to do so.
- Complete mandatory data protection and information security training and refresh it at the intervals set by the University.
- Comply with applicable software licence terms and conditions, including those relating to Chest/Jisc agreements. Some licences permit academic use only and users must observe any restrictions that apply.
- Not infringe copyright or break the terms of licences for software or other material. The fact that material is accessible online does not mean it may be freely used, copied or redistributed.

5.4 Prohibited activities

The University network and IT facilities must not be used directly or indirectly for the creation, downloading, alteration, transmission or storage of:

- Material that is offensive, obscene or contains indecent images.
- Material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise individuals.
- Data that facilitates harassment, bullying or victimisation of any member of the University community, the public or third parties.
- Information that endorses discrimination on any basis including race, gender, religion or belief, disability, age or sexual orientation.
- Information or data with the intent to defraud or deceive.
- Information or data that advocates or promotes any unlawful act.
- Information or data that infringes the intellectual property or privacy rights of a third party or breaches the terms of any software licence.
- Material designed to bring the University, its staff, students, alumni or partners into disrepute.
- Information that may be used for the propagation of terrorism, radicalisation or acts against the state.

Where research legitimately involves any of the above categories, prior approval must be obtained through the Senate Research Ethics Committee and the Information Assurance Team must be consulted so that risks can be properly assessed.

Users must not deliberately use the University network for activities having, or likely to have, any of the following effects:

- Destroying, corrupting, altering or otherwise interfering with another person's data without consent or authority.
- Disrupting the work of another person or the functioning of the University network.
- Intentionally denying access to the University network, its services or facilities to other users.
- Deliberately or recklessly introducing malware, spyware, viruses or other malicious software.
- Causing a breach of good practice likely to damage the reputation of the University or its third parties.

Users must not:

- Use personal email accounts to conduct University business.
- Store personally identifiable information or commercially sensitive data on unapproved services, devices or equipment.
- Download University data containing personal or commercially sensitive information onto non-University or personal devices.
- Use unencrypted removable media or portable devices to hold University data.
- Gain or attempt to gain unauthorised access to the University network, restricted programs, research data or applications.
- Deploy data-interception, password-detecting, packet-sniffing or similar software or devices on the University network.
- Download or install any application, operating system component or files on University-managed devices without authorisation through a Security Exception.

- Disable, interfere with or alter security controls, screen locks, anti-virus software or other protective measures on University devices.
- Use another person's credentials to access any system or service, or share their own credentials with anyone.
- Attempt to impersonate another person or disguise their identity when using IT facilities.
- Forward personally identifiable information or commercially sensitive material outside the University except to approved third parties with whom a contract is in place.
- Set up automatic forwarding of University email to external email accounts.
- Remove equipment, information or data from University premises without appropriate approval.
- Copy or transfer University data onto unencrypted removable media.
- Attempt to monitor or intercept the communications of other users without explicit authority.
- Send spam or unsolicited bulk email.
- Deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables.
- Set up servers or network services without approval from the IT department.
- Connect or attempt to connect any third-party, personal or unauthorised device to the University network without prior approval from the IT department, including but not limited to internet of things (IoT) devices, smart speakers, network-attached storage, wireless access points and other network-enabled equipment.
- Damage, reconfigure or move University IT equipment without approval.
- Use VPN anonymisers, internet proxy bypass services or other tools designed to circumvent University network security controls or monitoring.
- Use any software or resources in breach of applicable licence terms, including Chest/Jisc agreements and any conditions published by the Combined Higher Education Software Team.

5.5 Artificial intelligence and generative AI

The University's requirements for the use of artificial intelligence and generative AI tools are set out in the University's AI Guardrails, available on the University intranet. All users must comply with the Guardrails when using AI tools for University purposes.

Under this policy, users must not enter University data, personal data or commercially sensitive information into any AI tool or service that has not been approved by the University for that purpose.

Users remain responsible for the accuracy, integrity and compliance of any work they produce or submit, regardless of whether AI tools were used in its preparation.

Additional requirements relating to AI use in research, teaching and assessment are set by academic Schools, departments and the University's academic regulations.

5.6 Personal use

The University permits limited and reasonable personal use of its IT facilities. Personal use is a privilege rather than an entitlement and may be restricted or withdrawn at any time.

Reasonable personal use is occasional use that does not interfere with a user's duties or studies, is minimal in volume and duration, incurs no cost to the University, does not consume significant IT resources, does not interfere with the work or studies of others, and creates no legal, security or reputational risk to the University.

University accounts, email addresses, IT facilities, payment methods and delivery addresses are provided for University business and study. They must not be used for personal purchases, personal financial transactions, or as the contact or registration address for private matters unconnected with a user's role or studies. A personal email account should be used for such purposes.

Use of a University email address remains appropriate for professional activity connected with a user's role, including professional body membership, conference and training registration, external committee and editorial work, and academic collaboration.

University accounts and mailboxes are University records. They may be monitored in accordance with section 7 of this policy, may be accessed during investigations, may fall within the scope of freedom of information or subject access requests, and are closed when a user's affiliation with the University ends. Access to any external account or service registered to a University address will be lost at that point and cannot be recovered.

Personal files, photographs and media must not be stored on University systems or devices. The University does not provide technical support for personal use and cannot guarantee the confidentiality of personal content accessed or transmitted via University systems.

Use of University IT facilities for non-institutional commercial purposes or for personal financial gain requires the explicit approval of the President.

Detailed guidance on what constitutes reasonable personal use, including guidance specific to staff and to students, is published on the University intranet and must be followed. Where a user is uncertain whether particular use is permitted, they should seek advice under section 8 before proceeding.

5.7 Leaving the University

When a user's affiliation with the University ends, they must return all equipment assigned or loaned to IT. All equipment purchased by or through the University remains the property of the University, including assets purchased from research grants. Users must not retain or attempt to use University credentials once their affiliation ends. Before any University-owned device is disposed of, repurposed, sent for repair or transferred to another user, IT must ensure that all data is securely erased in accordance with the University's procedures. Users must not dispose of University equipment independently and should contact the IT Service Desk.

5.8 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:

a. Chief Information Officer (CIO) and Deputy CIO

The CIO holds overall accountability for the implementation of this policy, supported by the Deputy CIO. Together they ensure that appropriate technical, procedural and governance measures are in place to support compliance, and they approve any exceptions to this policy.

b. Information Security Manager

Maintains this policy, oversees its application within the University's information security management system, provides expert advice and monitors compliance through audits, reviews and security assurance activities.

c. Information Governance and Security Group (IGSG)

Provides oversight, challenge and assurance for information security and governance matters, including policy approval, risk management and monitoring of compliance across the institution.

d. Line managers and supervisors

Ensure that users within their teams understand and comply with this policy, complete mandatory training and follow established procedures. Managers must notify IT immediately when staff or contractors change roles or leave the University so that access can be amended or removed promptly.

e. System owners and data owners

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

f. All users

All users must comply with this policy and use University information and systems in a lawful, ethical and responsible manner. Users are required to protect credentials, follow security guidance, report actual or suspected incidents without delay and respect the lawful freedom of speech and academic freedom of others when using digital platforms.

g. 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 and data-protection standards. Contract managers must ensure appropriate due diligence, risk assessments and data-processing agreements are in place.

6 Procedure

6.1 Access and authorisation

Access to University systems, applications and data is granted on a least-privilege basis and must be approved through the appropriate University process. Users may only access systems for which they have been authorised, and access rights will be reviewed periodically. Requests for additional access must be justified by business need and authorised by the relevant manager or system owner.

All University systems and services require multi-factor authentication (MFA). Users must enrol in MFA and authenticate using the University's approved methods. Systems and services must be compatible with and use the University's central authentication, single sign-on (SSO) and MFA services.

6.2 Information security incident reporting

All users must report actual or suspected information security incidents immediately to the IT Service Desk or through the University's incident-reporting channels. This includes the loss or theft of devices, malware infection, unauthorised access or any misuse of University systems. Incidents will be logged, assessed and managed in accordance with the University's Security Incident and Data Breach Management Policy.

6.3 Handling of restricted or sensitive information

Users must ensure that personal data, commercially sensitive information and research materials classified as restricted are stored, processed and transmitted only via University-approved systems. Where research involves security-sensitive or legally controlled materials, users must obtain prior approval through the Senate Research Ethics Committee and ensure appropriate safeguards are in place, following University guidance and legal requirements.

6.4 Software, applications and device configuration

Installation of software, applications, scripts or operating system components on University-managed devices is restricted and must follow the University's Security Exception or Change Control process. Users must not alter device security settings or introduce unapproved software. Personal devices used to access University systems must meet the University's security standards.

6.5 Use of cloud services and external platforms

Only University-approved cloud services may be used to store, access or share University data. Users must not transfer information to personal cloud accounts or unapproved external platforms. Any proposed use of third-party services must undergo appropriate due-diligence and risk assessment in line with University procedures.

6.6 Network and remote access

Remote access to University systems must use authorised methods. Use of the University network is subject to the JANET Acceptable Use Policy and any associated service terms. Users must ensure that devices used for remote access are secure, up-to-date and protected by University-approved controls.

6.7 Account lifecycle management

User accounts will be created, modified and disabled in accordance with the University's account-management procedures. Creation and termination of access are informed by the start and end dates in the Human Resources and Student Records systems. Line managers must notify IT immediately of staff or contractor changes so that access can be amended or removed promptly. Users must not retain or attempt to use University credentials once their affiliation ends.

6.8 Policy awareness and training

All users must complete mandatory information security and data protection training and must refresh this training at intervals set by the University. Acknowledgement of this policy is required for account activation and continued access to University systems.

6.9 Monitoring

The University monitors and records the use of its IT facilities for the following purposes:

- The effective and efficient planning and operation of IT facilities and services.
- Detection and prevention of infringement of these regulations.
- Investigation of alleged misconduct.

The University will comply with lawful requests for information from government and law enforcement agencies. All monitoring activity will be conducted 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 Monitoring, Logging and Audit Policy.

7 Advice and guidance

7.1 IT Service Desk

The first point of contact for general IT queries, technical support, reporting issues, seeking assistance with access, devices, passwords or security-related concerns.

7.2 Information Security Manager

Provides specialist advice on information security controls, acceptable use requirements, secure handling of data, risk assessments and any questions relating to compliance with this policy or the University's information security standards.

7.3 Data Protection Officer (DPO)

The office of the DPO offers guidance on UK GDPR and the Data Protection Act 2018, including how personal data should be collected, stored, processed and shared. The DPO must be consulted where processing activities involve personal data risks or require a DPIA.

7.4 Research Ethics Team

Provides advice on the approval of research involving sensitive, security-controlled or legally restricted materials, including the requirements for Senate Research Ethics Committee approval.

7.5 Line managers and supervisors

Users may seek guidance from their line manager where policy obligations relate to their role, responsibilities or working practices. Line managers are responsible for ensuring staff follow policy requirements.

7.6 Additional guidance and resources

Further information, technical standards, operating procedures and security guidance are available on the University intranet, including instructions on approved storage systems, device security requirements, secure collaboration tools and incident reporting.

Users are encouraged to seek advice whenever they are uncertain about their obligations. Early engagement reduces risk and ensures compliance with legal, regulatory and contractual requirements.

8 Failure to comply

8.1 Users

Any breach of this policy by a user may result in withdrawal of access to University systems, mandatory retraining or other corrective measures. 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.

8.2 Legal and regulatory obligations

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

8.3 Misuse of credentials or access rights

Using another person's credentials, sharing passwords, elevating privileges without approval or attempting to bypass security controls is considered a serious breach and may result in immediate suspension of access pending investigation.

8.4 Damage, loss or misuse of University property

Users may be held responsible for damage caused by negligence or misuse of devices, systems or data. The University reserves the right to recover reasonable costs arising from the unauthorised, negligent or malicious use of technology resources.

8.5 Cooperation with investigations

Users must cooperate fully with investigations into suspected breaches, including providing relevant information, access to University-managed devices or clarification where requested. Failure to cooperate may itself constitute a breach.

8.6 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.

9 Review

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

Risk management and continuous improvement

Risks related to information security and acceptable use will be recorded in the University risk register and reviewed quarterly. Findings from incidents, audits and management reviews will feed into continual improvement of the ISMS.

Policy information

Should you require further information regarding this policy or access to the policy in an alternative format, then please contact the *CIO, cio-office@citystgeorges.ac.uk*

Policy Title:	Acceptable Use Policy
Policy Version:	V 92

Primary Author:	Eric McIntosh
Related Policies:	
Accountable Authority:	Chief Digital Information Officer
Approving Authority:	Information Governance and Security Committee
Date of Approval:	June 2026
Policy effective from:	Immediate
Date of Review:	June 2027

Appendix

[*An appendix to a policy may be used to set out specific procedures, contact information, examples of how to comply, etc*]