July 2021

Information Technology

Director of Information Technology

Version 4.0

Acceptable Use Policy

ITPOL03

Academic excellence for
business and the professions

Contents

1. Overview

The University processes information in order to carry out its normal functioning. This may include confidential and personal information about businesses and individuals. Information is a valuable, costly, asset. Business continuance and academic progress is dependent on its integrity and continued availability. Steps will be taken to protect information assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. This policy forms part of an information security management system (ISMS) which is a living document in support of these activities.

The Acceptable Use Policy sets out a set of unacceptable behaviours in Section 5 and later defines to a lesser extent behaviour, which is permitted on City, University of London IT systems. By stating what is unacceptable, users are then in a better position to use the provided systems in an acceptable and reasonable way. If users are in any way confused as to their responsibilities, they should seek guidance from the IT Service Desk.

2. Scope and applicability

This policy applies to staff, students, alumni, contractors, consultants, temporary and visiting staff, including interns, retired staff, honorary staff, volunteers and other workers of the University, including all personnel affiliated with third parties who interact with the information held by the University in all its forms and its related information systems. This includes, but is not limited to, any systems or data attached to the University computer or telephony networks, systems supplied by the University or communications sent to or from the University.

This policy applies to all people and assets in the execution of the original and supplemental University charters where pertaining to IT. This policy is reviewed, maintained and updated by the Information Security Manager. This policy will be reviewed, at minimum, annually.

3. Normative references, subsidiary controls

- This document forms part of an ISO/IEC27001 aligned ISMS
- Controls A6.2.1, A8.3, A9.1, A9.3.1, A9.4 of ISO/IEC27002 are applicable
- Legislation including but not exclusively: GDPR 2018, Data Protection Act 2018, Computer Misuse Act, Human Rights Act, Regulation of investigatory powers act 2000, the Terrorism Act (2006)
- Lawful Business Practice Regulations 2000 and general principals of employment law apply
- All university IT security policies form the one aligned ISMS suite governed by the Information Security policy (ITPOL01)
- The Director of IT shall oversee the implementation of information security controls and approve subsidiary policies.

4. Terms and definitions

For the purpose of this document, the terms and conditions given in ISO/IEC 27001 apply.

Standard IT taxonomy is used.

5. General policy

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

5.1 The University Network must not be used directly or indirectly by a person for the creation, downloading, alteration, transmission or storage of:

5.1.1 Any material which may be considered offensive, obscene or contain indecent images.

5.1.2 Material which may be considered defamatory, threatening, discriminatory, extremist or which has the potential to radicalise the individual or others. See section 5.1.10.

5.1.3 Any data which may be used to facilitate harassment, bullying and/or victimisation of a member of the University, public or third party.

5.1.4 Any information or data which endorses discrimination on any basis be that race, gender, religion or belief, disability, age or sexual orientation. Information containing this content for research purposes must be approved by the Senate Research Ethics Committee.

5.1.5 Any information or data with the intent to defraud or deceive.

5.1.6 Any information or data which advocates or promotes any unlawful act. Information containing this content for research purposes must be approved by the Senate Research Ethics Committee (UK law prevails).

5.1.7 Any information or data which infringes the intellectual property or privacy rights of a third party.

5.1.8 Any electronic or physical material which is designed to or will bring the University or its staff, students, alumni or partners into disrepute.

5.1.9 Any information that may or could be used for the propagation of acts of terrorism or against the state and radicalisation. Information containing this content for research purposes must be approved by the Senate Research Ethics Committee and notified Information Compliance.

5.2 The University network must not be deliberately used by a person for activities having, or likely to have, any of the following effects:

5.2.1 Destroying, corrupting, altering or otherwise interfering with another person's data without consent or authority to do so.

5.2.2 Disrupting the work of another person or altering the functioning of the University network.

5.2.3 Intentionally denying access to the University network, its services and facilities to other users by malice or forethought.

5.2.4 Causing a breach of good practice likely to damage the reputation of the University or its 3rd parties.

5.2.5 Where the University network is used to access another network or service, such as JANET, that organisation's Acceptable Use Policy must be respected and adhered to.

5.3 Users must not:

5.3.1 Use personal email accounts to conduct University business.

5.3.2 Store data which contains personally identifiable information or commercially sensitive data on/ in unapproved services or equipment.

5.3.3 Download City data containing personally identifiable or commercially sensitive information onto a non-City or personal device.

5.3.4 Use any form of unencrypted media or any other portable device, to hold City data. Exemptions may apply to this clause in some circumstances, please consult flexible working guidance on staff hub for the most up to date information.

5.3.5 Gain or attempt to gain unauthorised access to the University network.

5.3.6 Gain or attempt to gain unauthorised access to restricted programs, research data or applications held on the University network.

5.3.7 Deploy data-interception, password-detecting, packet sniffing or similar software or devices on the University network.

5.3.8 Users may not download or install any application, operating system or files for later installation on University devices; except those users who are specifically authorised by a Security Exception.

5.3.9 Carry out activities which may be seen to be intentional or reckless to introduce any form of spyware, computer virus or other potentially malicious software.

5.3.10 Attempt to disable screen locks or similar devices provided to protect systems.

5.3.11 Disable, interfere with or alter anti-virus on University devices.

5.3.12 Use anyone else's credentials to access the network or any other service that requires a logon.

5.3.13 Share their network username and password with anyone.

5.3.14 Forward any personally identifiable information as defined by GDPR or commercially sensitive material received via the City network. Excepting approved 3rd parties with whom the University has a contract in place.

5.3.15 Remove equipment, information or data from University premises without appropriate approval.

5.3.16 Copy or transfer any data on to unencrypted removable media.

5.4 Users **must:**

5.4.1 Take responsibility for protecting their username, password / passphrase.

5.4.2 Users must ensure applications and systems are up to date on the devices they are responsible for and respond promptly to any requests from IT to update their devices if necessary.

5.4.3 Make themselves familiar with the University Information and Data protection, Security policies and procedures.

5.4.4 Raise immediately if they detect, suspect or witness an incident that may be an information security breach. This should be done in accordance with the information provided on the Staff Hub. https://staffhub.city.ac.uk/information-technology/data-protection/data-breaches

5.4.5 Take precautions to protect all computer media and portable computers (e.g. walking with laptops opened and unlocked or left on display such that it would encourage an opportunist theft).

5.4.6 Comply with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and any other legal, statutory or contractual obligations that the University informs them is relevant.

5.4.7 All requests to use and research sensitive material (as defined by GDPR) at the University, including material relating to terrorism and extremism must be approved through the University's Senate

Research Ethics Committee and storage registered with the Research Ethics Office. Information Assurance Team must be contacted so the risks may properly be assessed.

5.4.8 Only use City approved storage systems to hold and store university data. Staff are reminded data may not be downloaded to their personal devices.

5.4.9 Ensure that any work, research or project undertaken using Personally Identifiable Information has either a Threshold Test or DPIA in force to cover the use of that information.

5.4.10 Understand their use of the University network may be monitored in line with City policies and where is a lawful basis to do.

5.5 When a user leaves the University they **must**:

5.5.1 Return all equipment assigned or loaned to them to their manager. All equipment purchased by City remains the property of City, this includes assets purchased from research grants.

5.5.2 Return any and all equipment assigned or loaned to them; delivery or collection will be arranged as appropriate. Staff are reminded equipment sourced via City IT remains the property of City, even if purchased from research grants.

6. Roles and responsibilities

All users of information systems are responsible for the security of data in their charge and care, it is their duty to ensure University systems are used appropriately and securely. Any person who suspects misuse of University systems should report the matter to their manager, supervisor or IT Service Desk without delay.

7. Compliance

7.1 Compliance measurement

The Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, video monitoring, and feedback to the policy owner.

7.2 Exceptions

Any exception to this policy must be approved by the Director of IT in advance.

7.3 Non-compliance

Any reckless or wilful conduct by any person or persons using City, University of London's network and computer systems which undermines this policy or puts at risk the security of data may result in disciplinary action being taken against them. All such cases will be fully investigated according to the University's disciplinary procedures and may be reported to the regulatory authorities.

In the case of a criminal offence being committed, City, University of London will involve the appropriate authority.

8. Risk management

Risk management for each department / School is defined within their Risk Management Policy.

9. Policy review

This policy will be reviewed by the process owners and updated alongside the security operating procedures on a regular basis, not to exceed 12 months.

10. Process owners

The Director of IT

11. Review schedule

This policy, and its subsidiaries, shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations by the Information Security Manager and the Information Security Committee. Additional regulations may be created to cover specific areas as required.

Document control

Change history			
Version	**Date**	**Author**	**Details of change**
1.0	30/10/2019	M Cann	Changed to live.
2.0	30/3/2020	M Cann	Added section 5.4.9 – OneDrive.
3.0	15/7/2021	M Cann / E McIntosh	2021 Reviewed. Changed to version 3.
4.0	18/2/2021	M Cann	Changes to 5.3.4 added 5.4.9 Changed to version 4

Document approval	
Approving Committee	**Approval Date**
ExCo	**28/10/2019**

Document review		
Reviewer	**Role**	**Review Date**
Russell Best	Systems & Operations Manager	16/7/2021
Claire Priestley	Director of IT	24/10/2019
Eric McIntosh	Joint Interim Director of IT	15/7/2021
M Cann	Information Security Manager	18/2/2022