October 2019

Information Technology

Director of Information Technology

Version 1.0

Conditions of Use Policy

ITPOL02

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.

1.1 This policy details the conditions which apply to all computers and networks at City, University of London.

1.2 This policy should be read in conjunction with the IT Information Security Policy, along with the JANET Acceptable Use Policy.

1.3 All users should be aware that by registering with City or by using the City network you have agreed to abide by all Information Security Policies.

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 set 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 A.5.1.1, A.6.1.1, A.7.1.2, A.7.2.3, A.8.1.3, A9.1.2, A.12.2.1, A.12.4.1, A.12.4.2, A.12.5.1 and A12.6.2 of ISO/IEC27002 are applicable
- 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 Resource usage

Facilities provided by City are intended to be used to further the aims and objectives of the University. A reasonable amount of personal use is permissible; however, priority must be given for the intended use.

All users must abide by City's Conditions of Use policy as well as external network's conditions, including JANET, who have their own Acceptable Use Policies.

5.1.1 All users must confirm with the IT Service Desk before installing any software. Licence conditions may limit software usage and could incur additional licence costs.

5.1.3 Using another user's username and password with or without their permission is strictly forbidden.

5.1.4 External resources (e.g. journals and software) that are accessed on the University's computing systems and networks have their own terms and conditions of use which require adherence.

5.2 Potential for harm

Certain activities while not, of themselves, necessarily illegal or damaging are restricted because they pose a risk of damage; financial or reputational risk to the University. The following list is not exhaustive:

- It is forbidden to store or publish within Moodle any information or data that would breach copyright laws.
- Care must be taken not to imply that a personal statement describes University policy
- Defamatory statements must be avoided, especially in public messages (webpages newsgroups, bulletin boards and mailing lists).

5.3 Investigation and enforcement

City maintains the right to monitor and log network activities. The following are examples of this monitoring:

- Usage of workstations, laptops and mobile devices
- Access to webpages
- Access to software
- Volume of data transfers
- Quantity of email

- Access to services, cloud storage and data sizing.

In most cases, the primary purpose of such logging is for fault investigation and capacity planning. Anomalies will prompt investigations of possible breaches of the Conditions of Use policy. Any of the information available can and will be used as evidence of possible misuse.

When required and not forbidden in law, further information may be collected in these cases. IT on behalf of the University reserves the right to:

- Inspect and store network traffic between any device connected to the network and any other internet address;
- Inspect and store the content of files held on any system managed by IT and on any system connected to the campus network;
- Inspect email and hold copies, both incoming and outgoing. Activate litigation holds and investigate as required;
- Automated filters are fitted in the email systems to prevent and detect virus, phishing and malware. Contaminated emails will either be cleansed or deleted dependent upon the nature of the threat posed;
- In the event of a virus or malware event occurring IT reserves the right to delete emails, files and lock accounts to contain and restrict the onward passage and growth of the malware;
- In the event of account misuse IT reserves the right to suspend accounts;
- Software monitoring is regularly undertaken to confirm systems are adequately licenced. IT reserves the right to uninstall any software not licenced or which poses a threat to University systems.

5.4 Regulation of Investigatory Powers Act 2000 (RIPA)

IT draws to the attention of all users of the University's data network; under RIPA their communications may be intercepted and inspected as permitted by legislation. The legislation allows the University to intercept without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use. The University does not need to gain consent before intercepting for these purposes. Staff and students of the University are hereby advised that interceptions may take place.

As IT have always had the authority to carry out certain monitoring activities in order to ensure the correct operation and security of the network and related systems, this is not seen as a change in practice. IT in this instance is acting on the University's behalf as the regulatory authority. Any other forms of monitoring of the network is expressly forbidden by the Network Code of Conduct, section 5.8.

5.5 Obscene Material

The University’s policy regarding obscene material on the internet was approved by Senate and Council in 2000 is underpinned by the following principles.

The University does not seek to lay down codes of moral behaviour in this area; however, it is bound by the law, by the conditions of use of the JANET network, and may be subject to UK Research and Innovation and Office for Students (OfS) sanctions.

Using the University's network to send, receive or store obscene material is a breach by the user of the terms of the Conditions of Use policy. Additionally, breaching them may render the University liable to criminal proceedings as a distributor of such material.

5.6 Security sensitive or extremism / terrorism material

There are a number of offences for accessing and distributing this type of information that apply to individuals and the University.

The Terrorism Act (2000) makes it an offence for an individual to collect or make a record of information of any kind likely to be useful to a person committing or preparing an act of terrorism; or to possess a document or record containing information of that kind (e.g. a terrorist training manual). Definition of terrorism is given in Section 1 of the Act at www.legislation.gov.uk/ukpga/2000/11/section/1.

The Terrorism Act (2006) www.legislation.gov.uk/ukpga/2006/11 outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Sections of the Terrorism Act also creates a risk of prosecution for those who transmit this material electronically. The storage of this information on a computer can prompt a police investigation.

The Counter-Terrorism and Security Act (2015) www.legislation.gov.uk/ukpga/2015/6 requires universities to "have due regard to the need to prevent people from being drawn into terrorism" (Section 26(1)).

All requests to use sensitive security material for research purposes at the University, including material relating to terrorism and extremism must be approved through the University's Senate Research Ethics Committee and use storage registered with the Research Office.

IT has procedures in place for security sensitive material to be stored within a limited circulation. Further detailed guidance will be provided by the Research Office and IT on a case by case basis. All external enquiries concerning access to security sensitive or extremism/terrorism material by staff and students should be directed to the Chair of the Senate Research Ethics Committee. If you come across security sensitive material whilst at the University bring it to the attention of the University's Information Security Manager or IT Service Desk.

5.8 Network Code of Conduct

Please note this section will shortly be subsumed into the User Acceptable Use Policy.

The data network at City, University London is a University resource which is installed and managed by IT on behalf of users. IT reserves the right to withdraw a user's permission to gain access to the network and facilities in the event of a breach of any of the following conditions. As per section 7, disciplinary proceedings may also be initiated against users in respect of any breach of the Code.

5.8.1 Prior permission and assistance must be sought from IT before any attempt is made to connect non IT supplied equipment of any description to the network. This excludes the wireless networks

5.8.2 All equipment must always be maintained and operated in such a manner that it does not interfere with or otherwise degrade the quality or performance of the network. Any malfunctioning equipment must be immediately disconnected from the network and reconnection may not be made until IT is satisfied about the performance of the equipment.

5.8.3 No attempt should be made to examine, copy or alter data on the network that is not legitimately destined for the user. Network scanning or monitoring software with the ability to observe data is prohibited. If such software can be shown to be essential for diagnostic purposes, then prior permission for use must be sought from IT, which if granted, applies only to temporary monitoring of the user's own data. Users should be aware that a breach of this condition is considered to be a serious matter and could lead to disciplinary proceedings being taken by the University. IT reserves the right to use such monitoring equipment to ensure compliance with this Code of Conduct.

5.8.4 Users must take adequate and reasonable measures to ensure that any equipment connected to the network is not left at any time in such a manner that unauthorised users can gain access to either the equipment or the network. Any suspected breaches of data security or confidentiality must be reported to IT immediately.

5.8.5 When accessing external sites, users should behave in a responsible manner with due respect to terms and conditions of use of those external sites.

5.8.6 Users should satisfy themselves that all the software they use is properly and adequately licenced and that copyrighted material is not shared or distributed via University systems unless a valid licence or agreement exists.

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 the Information Security Manager 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 handled internally and recorded on the appropriate risk register.

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

Director of IT.

11. Review schedule

This policy 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	Change version to live

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

Document review		
Reviewer	**Role**	**Review Date**
Russell Best	Systems & Operations Manager	15/10/2019
Claire Priestley	Director of IT	24/10/2019
M Cann	Information Security Manager	18/1/2022.