REGULATION 12
LIBRARY SERVICES AND INFORMATION TECHNOLOGY SERVICES

LIBRARY SERVICES

1. Entitlement to use Library Services

1. (i) All registered students, all current members of staff, including honorary staff, and all members of the City Alumni Network are entitled to use Library Services. Other persons may be granted access through reciprocal schemes or at the discretion of the Director of Library Services. Members of City Alumni Network may be charged an annual fee for use.

1. (ii) All users of Library Services are required to abide by the Code of Conduct and accompanying User Charter documents. Failure to do so may result in action taken under the University's disciplinary procedures.

2. Statutory provisions and other legislative requirements

2. (i) All users are required to comply with all statutory provisions and legislative requirements, including the Data Protection Act (1998); The Computer Misuse Act (1990); Copyright, Design & Patents Act (1988), including as amended by The Copyright and Related Rights Regulations 2003 and The Copyright and Rights in Performances Regulations 2014; Freedom of Information Act (2000); Regulation of Investigatory Powers Act (2000); Re-use of Public Sector Information Regulations 2005 and 2015; Criminal Justice Act (1994); Telecommunications Act (1984) and laws relating to obscenity and defamation.

3. Use of Online Resources

3. (i) Databases, online journals and other online resources are provided under licence to City, University of London. Licence conditions restrict use of these services to current, registered students and staff of the institution for the purpose of academic research only. All users must comply with the copyright holder's terms and conditions which vary according to the licence. The terms of individual licences are available on request.

4. Library Opening Hours

4. (i) City, University of London libraries shall open at such times as determined by the Library Leadership Team and are publicised on the City website. Announcements of any variation in opening times will be posted in advance on the City website.

5. Loan of Library Items

5. (i) Registered students and members of staff, and other eligible user groups, may borrow materials from the library. Loan periods vary according to the category of item and number of items permitted to borrow will vary according to the category of user. This information will be maintained and available on the Library Services website.

5. (ii) The following item types are not available for loan and may be consulted only in the library:

(a) Reference works
(a) Print journals and newspapers
(b) Theses
(c) Archive and Special Collection materials

5. (iii) All materials to be borrowed must be issued from Self-service machines or library service points. All City members are required to produce a valid student or staff registration card, as issued by Security Services. Retired staff members, alumni and registered external members must obtain a valid library card from the relevant office.

5. (iv) Returns:

All items must be returned at self-service machines, service desks or return points. Items must be returned on or before the last date notified at the time of issue or renewal. Charges for overdue items shall be levied at a rate determined by Library Services. Charges are levied to protect both the user and Library Services from loss and inconvenience through carelessness or lack of consideration on the part of individual borrowers.

5. (v) Renewals:

Certain items may be renewed for a further period if not required by another user.

5. (vi) Requests:

Requests for items on loan to another user should be made online via CityLibrary Search. The requestor will be notified when the item has been returned and it will be held for collection for a specified period. Borrowers will be advised of any change to the due date of items borrowed by email notification.

5. (vii) Interlibrary Loans:

Requests for loans of materials from other libraries should be made via the relevant form. Such loans are subject in each case to the conditions imposed by the library providing the loan and a charge per request will apply.

5. (viii) Lost or damaged books:

The loss of or damage to borrowed material must be reported immediately. The person in whose name it is borrowed is responsible for the cost of replacement or repair.

6. Photocopying

6. (i) Use of reprographic equipment must comply with the provisions of the Copyright Act and the Copyright (Library) Regulations currently in force, copies of which may be seen in the Library.

7. General

7. (i) Any disorderly or improper conduct or breach of the regulations will render the person concerned liable to suspension from the user of Library Services and action under the University disciplinary procedures.

7. (ii) Sections 8-11 of this Regulation (below) relating to the use of Information Technology Services apply to all use of IT hardware and software at City, including the use of IT hardware and software in library spaces.

7. (iii) Such additional rules as Library Committee, reporting to City's Executive Committee, shall from time to time approve will be posted on the Library Services and City website. Library Services Code of Conduct documents will be updated in a timely manner to reflect changes.

INFORMATION TECHNOLOGY SERVICES

8. Entitlement to use Information Technology Services

8. (i) All registered students and all current members of staff , including honorary staff, are entitled to use City, University of London's IT systems, which are institutional resources installed and managed centrally by Information Technology (IT).

8. (ii) Staff and students should be aware that registering with City, University of London you agree to abide by IT and Information Compliance policies, in particular the Information Security Policy; City's Acceptable Use Policy; JANET's Acceptable Use Policy; City's Conditions of Use and City's Network Code of Conduct.

8. (iii) IT Conditions of Use (including Network Code of Conduct): these form part of City's conditions of employment and student regulations. Breach of these conditions, particularly in relation to data protection and obscenity, may lead to disciplinary action. More serious breaches may be considered under gross misconduct. The Conditions of Use are reviewed annually.

9. IT Conditions of Use including Network Code of Conduct (summary of main points)

9. (i) Statutory requirements: users of City's IT network and IT systems are required to comply with statutory requirements. Particular care is needed to avoid breaching the following legislation Computer Misuse Act 1990;Copyright, Design and Patents Act 1988 as amended by The Copyright and Related Rights Regulations 2003 and The Copyright and Rights in Performances Regulations 2014; Counter-Terrorism and Security Act 2015; Criminal Justice Act 1994; Criminal Justice and Public Order Act 1994; Data Protection Act 1998; Defamation Act 2013; Freedom of Information Act 2000; Obscene Publications Acts 1959 and 1964; Privacy and Electronic Communications Regulations (PECR) 2003; Regulation of Investigatory Powers Act 2000; Telecommunications Act 1984; Terrorism Acts 2000 and 2006

9. (ii) Network Code of Conduct: users of City's IT network and IT systems must comply with the following conditions: Connection of equipment to network: prior permission must be sought from IT before any attempt is made to connect equipment of any description to the network. Forms for this purpose are available from IT and they must be fully completed and signed before being returned. If a connection request is approved, IT will perform the installation, with the cost to be borne by the user.

(a) Changes to the network: IT must be notified of all material changes including upgrades of hardware and software to permitted equipment. In particular, this includes changes to network addresses and network protocols.
(b) User email addresses: all users are required to provide IT with an email address at which they can be contacted. This address must be regularly checked for email and relevant messages responded to in a timely fashion. IT will provide an email address if required.
(c) Maintenance of IT equipment: all equipment must be maintained and operated at all times in such a manner that it does not interfere with or otherwise degrade the quality, performance of the network. On receipt of notification from IT, 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.
(d) Upgrades to the network: when requested to by IT users must disconnect specified equipment in order for upgrades, preventative maintenance or repairs to be effected to the network.
(e) Network monitoring: no attempt should be made to examine, copy or alter data on the network that is not legitimately destined for the user. In particular, network monitoring software having the ability to observe data on the network should not be used. 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 users 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 institution against the user. IT reserves the right to use such monitoring equipment to ensure compliance with this Code of Conduct.
(f) IT security and data breaches: users must take adequate 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.
(g) Use of external sites and networks: when accessing external sites and networks, users should behave in a responsible manner with respect to the use of any networks and systems used and acceptable use policies i.e. JANET acceptable use policy. This includes - but is not limited to - avoiding times of peak loading, heavy usage for trivial purposes, and use of false identification. Priority - especially at peak periods - must be given for the intended use.

9. (iii) Conditions of Use: City’s IT facilities are intended to be used in the furtherance of the aims and objectives of the institution. A reasonable amount of personal use is permissible – but the following expectations about the use of City IT network and IT systems apply:

(a) External resources and licences: a number of external resources are accessible by users of City's IT systems and network. Licence conditions on these resources may limit the nature of usage and must be followed.
(b) Commercial activities: work of a commercial nature, or for reward, and including web sites for external organisations requires prior written permission.
(c) Non-members of City: provision of any IT service to non-members of City requires prior written permission.
(d) Usernames and passwords: use of another user's username and password- with or without their permission - is forbidden. It is considered misuse by both lender and borrower.

(e) Password security: password security is key to ensuring your account is not misused. Take care of your password – do not share it or email it to anyone and avoid writing it down.
(f) Obscene or security sensitive material: users are not permitted to transmit onto the network obscene or security sensitive material without the permission of the Senate Research Ethics Committee, who will then formally notify IT that approval has been granted. See Security Sensitive Research policy on the Research Ethics section of City's website and the policies on obscene and security sensitive information outlined in City's IT Conditions of Use.
(g) Copyright: the storage or publication of information (including on web sites) intended to breach copyright is forbidden. Some copyright material may be used for teaching – (see copyright guidance on City's website).
(h) Personal statements: take care to avoid personal statements being described as institutional policy.
(i) Defamatory statements: defamatory statements, especially in "public" messages (web pages newsgroups, bulletin boards, and mailing lists) should be avoided.
(a) Use of open shares: Microsoft Windows operating systems allow the user to set up directories so that they can be shared with other Windows users. The guidance within the Windows Help system does not make explicitly reference to securing these files and as a consequence, the directories are often left entirely open and visible to other network users. The data contained in these shared areas is available to anyone on the City network. The use of these shares is bad practice, and if personal data is shared, this contravenes the Data Protection Act and renders City open to prosecution. If any open shares are discovered that contain personal data, it will be treated very seriously and may lead to disciplinary action. See policy on open shares in Conditions of Use.

10. Investigation and Enforcement

10 (i) Routine logging and monitoring of IT network and systems: certain activities on the network and centrally provided systems are routinely logged and/or automatically monitored. These include usage of workstations; access to web pages; access to software; volume of data transfers; quantity of email; scans for obscene material (See Policy on Obscene Material in Conditions of Use) and scans for vulnerable shared directories (open shares) (See Policy on Open Shares in Conditions of Use).

10 (ii) Purpose of logging: the primary purpose of such logging is for fault investigation and capacity planning, but anomalies may prompt investigation of possible breaches of the Conditions of Use and the information is available when evidence of potential misuse is needed.

10 (iii) Investigation of specific complaints: a complaint may have been from the managers of remote sites and networks, from users, from the police, or as a result of an investigation prompted by an anomaly in routine monitoring. In these cases, where not forbidden by law, IT reserves the right to:

(a) Inspect network traffic between a user's machine and any other address(es)
(b) Inspect - possibly via an automated search - the content of files held on any system managed by IT and on any system - even privately owned - that is, or has recently been, connected to City's network.
(c) Inspect email, both incoming and outgoing. Automated filters are installed to intercept the transmission of email to remove viruses and identify potential spam email.

Further restrictions may be employed in the event of warnings about harmful software (e.g. viruses and worms) or security problems being received.

(d) Cut off access (either by disabling logins or by disconnecting from the network) where it is considered advisable to prevent further misuse.

(e) Examine any City owned IT equipment for unlicensed software and test the security of any IT equipment connected to City's network.

10 (iv) Confidentiality of information collected: except where it provides evidence of a breach of these conditions, of serious criminal activity, or of significant costs to City, information acquired during any monitoring will be kept strictly confidential to those directly involved in the investigation. In the case of serious criminal activity the information will be made available to the police.

10 (v) Breaches of Conditions of Use: serious breaches of Conditions of Use and Network Code of Conduct will be handled by City's Disciplinary Procedures and particularly in relation to data protection and obscenity, may lead to disciplinary action. More serious breaches may be considered under gross misconduct. Less serious cases by summary action by a senior member of IT (in this case the alleged offender may insist on the use of the City's Disciplinary Procedures as an alternative). When summary action is taken, the punishment is normally a suspension of permission to use the IT facilities and network.

11. Regulation of Investigatory Powers Act (RIPA) 2000

11 (i) Statutory notification under RIPA to all users of City's IT network:

Your communications may be intercepted and inspected as permitted by legislation. The legislation allows City to intercept without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance, and detecting crime or unauthorised use. City does not need to gain consent before intercepting for these purposes, although staff and students are advised that interceptions may take place.

11 (ii) IT staff have the authority to carry out certain monitoring activities in order to ensure the correct operation of the network and related systems. This does not imply that all communications are monitored but serves to advise all users that they may be for the purposes outlined above. It should be noted that IT is acting on City's behalf as the regulatory authority in this instance. Any other monitoring of the network is expressly forbidden by the Network Code of Conduct.

Approved by Senate 3.12.75; 9.5.79, 6.12.00
Approved as a Regulation (Senate) 4.7.07
Approved by Chair's Action (Senate) 24.08.16
Approved as a Regulation (Senate) 12.07.17