# City University of Hong Kong

# Policy on Use of IT Services and Facilities

*(revision approved by the Information Strategy and Governance Committee on 16 March 2015)*

## A. Purpose

1. The City University of Hong Kong (CityU) recognises the importance of information technology (IT) in teaching, learning, research and administration. Various *IT Service Providers* within the University provide and manage an extensive range of *IT Resources* to support the mission of the University. Use of these *IT Resources* is governed by a set of *IT Policies and Regulations* (which includes this document), the laws of the Hong Kong Special Administrative Region (HK SAR), and the laws of other country where the *IT Resources* are located or hosted.

## B. Scope

1. The following policy statements must be observed by all (i) users of the *IT Resources* including students, staff, alumni, applicants, guests, visitors and any other persons who have been given access to *the IT Resources*, and (ii) by the respective *IT Service Providers*.

## C. Statement

1. Each user is given an Electronic ID (EID) to access the *IT Resources*. Users are responsible to maintain the security of their EIDs and passwords and thus held accountable for all activities performed under their EIDs.

2. To safeguard the University operations supported by the *IT Resources*, users may be asked by the respective *IT Service Providers* to change their passwords regularly, or in some urgent cases (e.g. under hacker's attack) immediately, on short notice.

3. Users are expected to use the *IT Resources* with courtesy, respect and integrity.

4. Users must not interfere with the work of other users or alter the integrity of the *IT Resources*.

5. Users must use the *IT Resources* responsibly and in adherence to the mission of the University. Users must not use them for any illegal or unauthorised purpose such as conducting commercial activities for unauthorised personal financial gain.

6. Users are expected to use electronic communication (email, messaging, web content, social media, etc.) in an ethical and responsible manner and in compliance with general guidelines based on common sense, common decency, and civility applicable to the networked computing environment.

7. Users must observe the Crimes Ordinance and neither attempt to gain unauthorised access to data or information, nor breach any security measures imposed on any of *the IT Resources*. Any violation on using such *IT Resources* may be reported to the related law enforcement agencies.

8. Users must observe the Copyright Ordinance. Software or electronic contents without proper license are not allowed to be stored or used in the *IT Resources*. Any such violation may be reported to the related law enforcement agencies.

9. Users must adhere to the Personal Data (Privacy) Ordinance in all activities involving collection, processing, use, and proper disposal of personal data. Any violation of the Ordinance will be reported to the Data Protection Officer of the University.

10. Individual *IT Resources,* due to its specific application or environment, may have additional regulations which users must also observe.

11. Users agree that the respective *IT Service Providers*, entrusted by the University to maintain the health and proper use of the *IT Resources*, have the right to inspect, monitor, remove, block or disclose any data or information either stored or communicated via the IT services if there is compelling evidence of (i) violating either the policies and regulations of the *IT Service Providers* or any applicable laws and regulations from all applicable jurisdictions, or (ii) adversely affecting the normal functioning of the IT services or normal use of the *IT Resources*.

12. All users and departmental *IT Service Providers* have the responsibility to report to *Central IT* on any non-compliance of the prevailing *IT Policies and Regulations*. *Central IT* will treat all such non-compliance as IT incidents so that they will be timely reviewed, and the corresponding preventive measures, if any, be adopted.

## D. Enforcement

1. Failure in complying with the *IT Polices and Regulations* may result in immediate suspension or termination of accessing some or all *IT Resources* provided to the violators without prior notice. Such suspension or termination will only be lifted or revoked after remedial action has been taken to the satisfaction of the *IT Service Provider*, and if necessary, of the respective line management. Any student or staff who is alleged to have violated any IT policy or regulation may be subject to further disciplinary action if any, in accordance with the Student Disciplinary Procedures or Staff Disciplinary Procedures, respectively. *Central IT* and/or respective *IT Service Providers* may impose additional penalties if necessary.

## E. Terms and Definitions

1. **Central IT**
   *Central IT* consists of the Office of the Chief Information Officer (OCIO), the Computing Services Centre (CSC), and the Enterprise Solutions Office (ESU).

2. **CSC Teaching Studio Areas**
   These areas include all teaching studios and classrooms operated by CSC, including but not limited to the various CSC teaching studios in AC2.

3. **Data Custodians**
   *Data Custodians* define, implement, and enforce data management policies and procedures within their specific subject area and business domains; these include mainly the various University administrative offices.

4. **Electronic University Data**
*Electronic University Data* refer to all data and information collected, maintained, or used in the University's information systems.

5. **Email Services**
The *Central IT* offers the following *Email Services:*

| Email domain name | Type |
|---|---|
| Staff | |
| @cityu.edu.hk | University account |
| @um.cityu.edu.hk[#1] | |
| @staff.cityu.edu.hk[#1]<br>@GApps.cityu.edu.hk[#2] | Supplementary account |
| Students | |
| @my.cityu.edu.hk[#1] | University account |
| @GApps.cityu.edu.hk[#2] | Supplementary account |
| Alumni | |
| @my.cityu.edu.hk[#1]<br>@alumni.cityu.edu.hk | Courtesy email service account |
| Retired staff | |
| @friends.cityu.edu.hk[#2] | Courtesy email service account |

*[#1] Services hosted by Microsoft.*
*[#2] Services hosted by Google.*

Obsolete email services:

| Email domain name | User | Type |
|---|---|---|
| @mslive.cityu.edu.hk[#1] | Staff, Students, Alumni and Long-serving Staff | University account/ courtesy email service account |
| @student.cityu.edu.hk | Students | University account |

6. **Regulations on IT Services and Facilities**
The *Regulations on IT Services and Facilities* include*:*
(1) CityU Electronic Mail Regulations
(2) Campus IT Network Regulations
(3) Electronic University Data Regulations
(4) CSC Teaching Studio Areas Regulations
(5) Notebook Computer Daily Loan Scheme Regulations

7. **IT Policies and Regulations**
The *IT Policies and Regulations* include the "Policy on Use of IT Services and Facilities" (i.e. this document) plus the 5 regulation documents in the *Regulations on IT Services and Facilities.*

*8.* **IT Resources**
*IT Resources* include various IT services, manpower, information, data and facilities to support the mission of the University.

9. **IT Service Providers**
*IT Service Providers* include various University departments and offices, including the *Central IT*, that provide and manage *IT Resources.*

## F. Related Policies and Regulations

1. This document is only part of the *Central IT*'s set of *IT Policies and Regulations.* Please refer to the "Definition" section of this document for a complete list of documents in this set.

2. The *IT Policies and Regulations* may be revised from time to time as necessary without prior notice.

## G. Contact Information

1. For questions about this document, please contact the Office of the Chief Information Officer (OCIO) at cio@cityu.edu.hk.

# City University of Hong Kong

# Regulations on Use of IT Services and Facilities
# (1) CityU Electronic Mail Regulations

*(revision approved by the Information Strategy and Governance Committee on 16 March 2015)*

## A. Purpose

1. The acceptable use and unacceptable use of the *Email Services* and related violation penalties, if any, are governed by the "Policy on Use of IT Services and Facilities", "Campus IT Network Regulations", "Electronic University Data Regulations", "Information Security Policies and Standards" and additional regulations defined in this document.

2. The use of externally hosted email services are further governed by the Terms and Conditions (T&C), if any, of their respective service providers.

## B. Scope

1. All users of University provided *Email Services* are subject to regulations defined in this document.

## C. Statement

1. All emails sent from the staff's computer accounts via services managed by *Central IT*, including replies and forwarded email, should contain the standard disclaimer of the University:

   *"This email (including any attachments) is for the use of the intended recipient only and may contain confidential information and/or copyright material. If you are not the intended recipient, please notify the sender immediately and delete this email and all copies from your system. Any unauthorized use, disclosure, reproduction, copying, distribution, or other form of unauthorized dissemination of the contents is expressly prohibited."*

2. Users must not use email for activities such as defamation, abuse, harassment, obscenity, threats or otherwise violating the legal rights (such as rights of privacy and publicity) of others.

3. Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless expressly authorised to do so.

4. Users must not impersonate another person or entity, or falsify or delete any author attributions, legal or other proper notices or proprietary designations or labels of the origin or source of software or other material contained in a file that is sent.

5. The *Email Services* shall not be used for purposes that can reasonably be expected to cause, directly or indirectly, either strain on any *IT Resources* or interference with others'

use of such *IT Resources*. For example, users must not send or forward chain-mail, mail-bombs or spam.

6. Users must not intentionally transmit any viruses, worms, defects, Trojan horses, or any items of destructive nature. They shall also protect their computers to avoid unintended transmission of the above.

7. Users must take necessary precautions to protect the confidentiality of personal or confidential information found in Email and its backups, archives, cloud storage or other electronic records stored.

8. According to the “Information Classification and Handling Standard”, email that contains any information that has been classified as “RESTRICTED” or “CONFIDENTIAL” must be encrypted for transmission and storage.

9. Users must follow the good practice to avoid activities that may affect the performance of the Email system and interfere with the work of others such as subscribing to list-servers, transmitting messages with large attachments or sending messages to a large group of recipients.

10. Users may use @cityu.edu.hk, @um.cityu.edu.hk, @my.cityu.edu.hk and @alumni.cityu.edu.hk *Email Services* for incidental personal purposes provided that such use does not (a) interfere with the University's operation; (b) interfere with the user's obligations to the University, or (c) incur noticeable costs to the University.

11. The *Email Services* must not be used as a kind of storage for University records. System backups for the *Email Services* are performed only for the purposes of disaster recovery, and of judicial discovery requests from law enforcement agencies of the Hong Kong SAR Government when contents of such backups may be legally admissible. Appropriate storage for retention and disposal of work-related email is the responsibility of the originator/recipient of the email. It is the responsibility of all staff to ensure that their email records are retained for the appropriate period, and are also deleted when appropriate in accordance with the record type.

12. To maintain the health of the *Email Services*, *Central IT* reserves the right to take any measures, subject to the prevailing rules on confidentiality, privacy and accountability stipulated by the respective IT Service Providers, to examine the message content, remove or reject any electronic messages that are considered harmful to the service.

13. In order to be able to effectively and speedily stop the delivery of any possible spam email, *Central IT*, upon receiving a number of complaints, will block further delivery of such or similar email at its discretion.

14. Direct marketing messages which are sent via the *Email Services* should follow the procedures about the use of personal data in direct marketing given under the University Code of Practice on Personal Data (Privacy) Issues and be compliant with the Unsolicited Electronic Messages Ordinance (UEMO) of Hong Kong.

## D. Enforcement

1. Failure to comply with any regulation defined in this document may result in penalties as described in the "Policy on Use of IT Services and Facilities."

## E. Terms and Definitions

1. A common set of terms and definitions used in the *IT Policies and Regulations* are defined in the "Policy on Use of IT Services and Facilities" document.

## F. Related Policies and Regulations

1. This document is only part of the *IT Policies and Regulations.* The "Policy on Use of IT Services and Facilities" contains a complete list of other documents in the *IT Policies and Regulations*.

2. The *IT Policies and Regulations* may be revised from time to time as necessary without prior notice.

## G. Contact Information

1. For questions about this document, please contact the Office of the Chief Information Officer (OCIO) at cio@cityu.edu.hk.

# City University of Hong Kong

# Regulations on Use of IT Services and Facilities
# (2) Campus IT Network Regulations

*(revision approved by the Information Strategy and Governance Committee on 16 March 2015)*

## A. Purpose

1. The proper use of the campus network and the violation of such use (including its related penalty, if any) are governed by the "Policy on Use of IT Services and Facilities", "Information Security Policies and Standards", the JUCC's "HARNET Acceptable Use Policy"[1] and additional regulations defined in this document.

## B. Scope

1. All users with access to the campus IT network are subject to regulations defined in this document.

## C. Statement

1. Users must not attempt to disrupt or degrade the performance of host systems, any device on the network, or any IT service delivered over the network.

2. Loopholes in network security systems or knowledge of special passwords etc. must not be used to gain access to any service or any resource on the network for which proper authorisation has not been given by *Central IT*.

3. Users who are aware of any problems on network security should report such to the CSC Help Desk.

4. Users must not create or distribute malicious software codes on the network, and should take all reasonable precautions to prevent such actions.

5. Users must not connect or disconnect networking equipment (e.g. bridges, routers, repeaters, protocol analysers, data loggers, transceivers, Wireless LAN device, etc.) to or from the campus network without proper authorisation from *Central IT*. All network changes made by departments to the campus network, including the information of the administrators involved and/or users affected (if applicable), need registration and/or updates, as appropriate, with *Central IT*.

---

[1] JUCC is the Joint University Computer Centre Limited and the HARNET Acceptable Use Policy can be found at http://www.jucc.edu.hk/harnet.html.

6. Users must not conduct network experiments on the campus network such as demonstrating network vulnerabilities, sniffing network traffic, generating network traffic which will lead to depletion of its available bandwidth, or setting up phishing sites, etc. unless proper authorisation has been given by *Central IT*.

7. All computers directly reachable from the Internet or Intranet (i.e. not connected to a private or standalone network) must use only those IP addresses/node names/domain names that are approved by *Central IT* in order to avoid conflicts which might result in disruption of normal operation of the campus network. Please refer to the "IP address registration" and "Domain Name System Policy and Guidelines".

8. Users must register in advance with *Central IT* (a) for any network server or communication link installed on campus through which the IT service, accessible by remote user, is offered, or (b) for any IT service that is offered to staff and students but hosted by external service providers.

9. Without prior approval from *Central IT*, users must not perform network scanning or port scanning on the campus network.

## D. Enforcement

1. Failure to comply with any regulation defined in this document may result in penalties as defined in the "Policy on Use of IT Services and Facilities."

## E. Terms and Definitions

1. A common set of terms and definitions used in the *IT Policies and Regulations* are defined in the “Policy on Use of IT Services and Facilities” document.

## F. Related Policies and Regulations

1. This document is only part of the *Central IT*’s *IT Policies and Regulations.* The “Policy on Use of IT Services and Facilities” contains a complete list of other documents in the *IT Policies and Regulations*.

2. The *IT Policies and Regulations* may be revised from time to time as necessary without prior notice.

## G. Contact Information

1. For questions about this document, please contact the Office of the Chief Information Officer (OCIO) at cio@cityu.edu.hk.

# City University of Hong Kong

# Regulations on Use of IT Services and Facilities
# (3) Electronic University Data Regulations

*(revision approved by the Information Strategy and Governance Committee on 16 March 2015)*

## A. Purpose

1. The proper access of *Electronic University Data* as well as access violations and related penalty, if any, are governed by the "Policy on Use of IT Services and Facilities" and additional regulations defined in this document.

## B. Scope

1. Access to *Electronic University Data* is restricted to authorised employees or other individuals for performing assigned duties. Such authorization will be withdrawn when a person's business needs for the data cease.

## C. Statement

1. Having been granted access to the *Electronic University Data*, users undertake to keep the data secure and confidential, and shall not disclose such information to any person without approval.

2. Users should avoid making any copies of data in paper or electronic form (including but not limited to PC, camera, telephone, PDA, USB, CD, memory cards, etc.). In cases where the making of a copy is necessitated by the nature of the work at hand, users must take proper security measures to protect the media and the content against damage, theft, fraudulent manipulation and unauthorised access. Any personal or sensitive data, such as student data, personnel data, or financial data, if stored on portable electronic storage devices, must be encrypted and kept under lock when not in use. All copies of data should be destroyed as soon as their use is no longer required. For electronic storage, the content must be removed from these media in a manner that will render the data unrecoverable.

3. Users are prohibited to transfer any data to any party without proper authorisation by the respective *Data Custodians*; and unless with prior approval from the *Data Custodian*, under no circumstances should data be (i) transmitted via any communication service or (ii) uploaded, stored, or presented onto any external or cloud site which is neither owned nor managed by the University.

## D. Enforcement

1. Upon consultation with or as advised by the respective *Data Custodian*, a user may be deprived of the access right to the concerned data at any time by the respective *IT Service Provider* without prior notice.

2. Failure to comply with regulations defined in this document may result in further penalties as defined in the "Policy on Use of IT Services and Facilities."

## E. Terms and Definitions

1. A common set of terms and definitions used in the *IT Policies and Regulations* are defined in the “Policy on Use of IT Services and Facilities” document.

## F. Related Policies and Regulations

1. This document is only part of the *IT Policies and Regulations.* The “Policy on Use of IT Services and Facilities” contains a complete list of other documents in the *IT Policies and Regulations.*

2. The *IT Policies and Regulations* may be revised from time to time as necessary without prior notice.

## G. Contact Information

1. For questions about this document, please contact the Office of the Chief Information Officer (OCIO) at cio@cityu.edu.hk.

# City University of Hong Kong

# Regulations on Use of IT Services and Facilities
# (4) CSC Teaching Studio Areas Regulations

*(revision approved by the Information Strategy and Governance Committee on 16 March 2015)*

## A. Purpose

1. The acceptable and unacceptable use of the facilities at the *CSC Teaching Studio Areas* and related penalties, if any, are governed by the "Policy on Use of IT Services and Facilities" and additional regulations defined in this document.

## B. Scope

1. All users of the facilities at the *CSC Teaching Studio Areas* are subject to regulations defined in this document.

## C. Statement

1. All users, upon request, must produce appropriate ID cards for inspection by the security guard or the CSC staff on duty.

2. A user at the *CSC Teaching Studio Areas* must:

   2.1. use only the workstation he/she has booked through the Computer Reservation System;
   2.2. use only his/her own account to book the workstation and use the workstation only for academic work;
   2.3. follow the instructions in front of each laser printer and observe best practice/guidelines in related website when using the laser printing service;
   2.4. return to the Service Counter all loaned equipment or manuals 15 minutes before the service closing time;
   2.5. leave the CSC immediately at its closing time, or at any other time when instructed to do so by the security guard or the CSC staff on duty;
   2.6. look after the personal belongings at all times and ensure to bring with him/her all his/her personal belongings including mobile devices, removable storage media, etc. before leaving the CSC;
   2.7. practise green IT (e.g. printing hard copy only when absolutely necessary, powering off the workstation after use, etc.), and
   2.8. report any malfunction of equipment to the Service Counter for repair.

3. A user at the *CSC Teaching Studio Areas* must not:

   3.1. cause any nuisance or disturbance to others (e.g. shouting, singing, playing music or computer game, etc.);
   3.2. install, alter, delete, or copy any software on computers provided by CSC;
   3.3. allow others to use his/her account(s) and CityU ID card;

3.4. use any equipment for non-academic related work (e.g. printing blank paper, election materials, etc.);
3.5. alter the location and connections of any equipment (e.g. power bar, network cable, monitor, keyboard, mouse, CCTV, etc.);
3.6. connect any device to the equipment in the *CSC Teaching Studio Areas* without prior approval by CSC;
3.7. in any way deface or damage any equipment, manual, or other property of CSC;
3.8. leave personal belongings unattended at any time;
3.9. eat, drink, or play any form of game, and
3.10. without prior approval from CSC, repair or attempt to repair CSC's equipment, or alter their hardware or software settings.

## D. Enforcement

1. Failure to comply with regulations defined in this document may result in penalties as defined in the "Policy on Use of IT Services and Facilities."

## E. Terms and Definitions

1. A common set of terms and definitions used in *IT Policies* are defined in the "Policy on Use of IT Services and Facilities" document.

## F. Related Policies and Regulations

1. This document is only part of the *IT Policies and Regulations.* The "Policy on Use of IT Services and Facilities" contains a complete list of other documents in the *IT Policies and Regulations*.

2. The *IT Policies and Regulations* may be revised from time to time as necessary without prior notice.

## G. Contact Information

1. For questions about this document, please contact the Office of the Chief Information Officer (OCIO) at cio@cityu.edu.hk.

# City University of Hong Kong

# Regulations on Use of IT Services and Facilities
# (5) Notebook Computer Daily Loan Scheme Regulations

*(revision approved by the Information Strategy and Governance Committee on 16 March 2015)*

## A. Purpose

1. The acceptable and unacceptable use of Notebook Computer Daily Loan Scheme (DLS) and related penalties, if any, are governed by the "Policy on Use of IT Services and Facilities" and additional regulations defined in this document.

## B. Scope

1. All users of the DLS are subject to regulations defined in this document.

## C. Statement

1. The DLS is provided to all full-time and part-time students of the main campus who may borrow notebook computers and use them for their studies within the campus. However, students who have already borrowed a computer under the Student Notebook Computer Long Term Loan Scheme ("LLS") are not entitled to reserve another DLS notebook computer in advance as stated in paragraph 2 below.

2. Students should reserve notebook computers through the Computer Reservation System available on the e-Portal. The DLS maintains a point system for reservation to ensure the Service is rendered in a fair and flexible manner. The Computing Services Centre (CSC) reserves the right to adjust these point levels when necessary and without prior notice.

3. Students who have not made any reservation may also borrow notebook computers if spare ones are available at the CSC DLS Counter.

4. Students must take the notebook computer assigned to them by the staff at the CSC DLS Counter.

5. Students are responsible to check the notebook computer once they obtain it from the CSC DLS Counter and must return any malfunctioned or damaged notebook computers to the DLS Counter within half an hour after the checkout.

6. Students must not lend the notebook computers that they have borrowed to others or ask someone else to return the notebook computers on their behalf.

7. Students must return the notebook computers on the same day of borrow. Before returning them, students should erase all data on the notebook computers to protect the privacy of their own data.

8. Students are solely responsible for any loss or damage of the notebook computers they have borrowed. Students will be charged the repair cost if the computer is found to be damaged

upon return. In the event of loss, students will be charged the replacement cost of the computer, assessed based on the original price and depreciation of the lost computer.

## D. Enforcement

1. Students who fail to return the notebook computers by the due time are subject to a fine of HK$100 per day including public holidays, and addition of extra point(s) thus lowering their loan priority.

2. If students fail to return the notebook computers or settle the payments due to damage, loss or late return, the Service to them will be suspended.

3. Failure to comply with regulations defined in this document may result in further penalties as defined in the "Policy on Use of IT Services and Facilities."

## E. Terms and Definitions

1. A common set of terms and definitions used in the *IT Policies and Regulations* are defined in the “Policy on Use of IT Services and Facilities” document.

## F. Related Policies and Regulations

1. This document is only part of the *IT Policies and Regulations.* The “Policy on Use of IT Services and Facilities” contains a complete list of other documents in the *IT Policies and Regulations*.

2. The *IT Policies and Regulations* may be revised from time to time as necessary without prior notice.

## G. Contact Information

1. For questions about this document, please contact the Office of the Chief Information Officer (OCIO) at cio@cityu.edu.hk.