City University of Hong Kong Policies on Use of IT Services and Resources

A. Purpose

The City University of Hong Kong (CityU, "the University") recognises the importance of information technology (IT) in teaching, learning, research and administration. With the use of software-as-a-service and cloud computing, various IT service providers now offer and manage an extensive range of IT services and resources within the University. Improper use of these resources, whether unintended or not, can have significant negative consequences for the University and its community. The use of IT services and resources is therefore governed by a set of CityU policies, principles, and regulations (including this document), the laws of the Hong Kong Special Administrative Region (hereafter "HKSAR"), and the laws of other countries where the IT services and resources are provided or hosted, or where users are located. Use of CityU IT services and resources is a privilege, not a right.

B. Scope

The following principles and policy statements apply to all users of CityU IT services and resources including students, staff, alumni, contractors, retired staff, applicants, guests, visitors and other persons who have been given access to the IT services and resources. By accessing the IT services and resources, users agree to comply with all applicable regulations (see Section A).

C. Principles

This document provides the framework for a set of policies and regulations (see Section G). In formulating these principles and regulations, the University relies on a set of guiding principles, which users must adhere to. Non-adherence will be considered as improper use of CityU IT services and resources.

Users of CityU IT services and resources:

- must act responsibly and in consideration of the rights of all others affected by them;
- must not harm any internal or external individuals or become a nuisance to them;
- must not harm the property or reputation of the University;
- should recognize and understand the ownership of the IT services and resources and not violate the corresponding ownership rights;
- should report any improper IT services or resources uses by other users;
- recognize the University's right to assure proper function of IT services and resources, even if this negatively impacts individual users or groups of users;

- recognize the University's right to enforce proper use behaviours, respond to violations, and impose penalties for improper use.

D. Policy Statements

1. Users are given Electronic ID or login accounts (hereafter collectively "EID") to access the relevant IT services and resources. Users will be held accountable for all activities performed under their EID. Users are therefore responsible for the safeguarding of their EID and its corresponding password(s).
2. To safeguard the University operations, users may be asked to change their passwords regularly, or in urgent cases (e.g. hacker compromised EID) immediately and without delay.
3. IT services and resources may require registration data and other information in order to operate. Users consent to the University's collection and use of this information subject to CityU's prevailing privacy policy.
4. Users shall not resell, rent, lease, loan, share, distribute, modify, or copy any portion of the IT services and resources, or access thereof, in whole or in part.
5. IT services and resources users must not interfere with the work of others or alter the integrity of the IT services and resources.
6. CityU IT services and resources are provided for academic uses (teaching, learning and research) and administrative uses, on the strict understanding that they are to be used solely for the University's intended purposes (i.e., teaching and learning, administrative activities, operations).
   6.1. 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. The University assigns all members a registered email address under CityU's domain addresses. This is the designated channel for official CityU communications. CityU members are responsible to regularly check their CityU email accounts for new communications.
8. Certain academic and administrative communications are deemed essential by the university for proper operation and informed academic dialogue. CityU members and/or users of CityU's communication systems and services (e.g., email users) cannot opt out from receiving these communications. The communications include, but not limited to, university announcements, service announcements, administrative messages, and CityU Newsletter.
9. Users must use the IT services and resources responsibly and adhere to the mission of the University.
10. Users must not use CityU IT services and resources for any unauthorised purposes such as conducting commercial activities for unauthorised financial gains.
11. Users must not use CityU IT services and resources for illegal purposes.

11.1. 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 services and resources. Any violation on using such IT services and resources may be reported to the related law enforcement agencies.

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

11.3. 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.

11.4. Specific IT services and resources, due to its specific application, environment or needs, may have additional regulations which users must also observe.

12. Users agree that the respective IT Service Providers, entrusted by the University to maintain the health and proper use of the IT services and 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 or normal use of the IT services and resources.
13. All users and departmental IT services and resources providers have the responsibility to report to Central IT on any non-compliance of the prevailing IT Policies and Regulations as soon as possible. Central IT will treat all such noncompliances as IT incidents so that they can be reviewed in a timely manner, and corresponding preventive measures, if any, be adopted.

E. Enforcement

Failure to comply with the IT Polices and Regulations may result in immediate suspension or termination of access to some or all IT services and resources provided to the non-compliant user. Suspension or termination may occur without prior notice and will only be lifted or revoked after remedial action has been taken to the satisfaction of the IT service provider(s), and if necessary, of the respective line management. Any user who is alleged to have violated any policy or regulation may be subject to further disciplinary action if any, in accordance with the University's disciplinary procedures. Central IT and/or respective IT service providers may impose penalties when deemed necessary, independent of any disciplinary procedures the University might invoke.

F. 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. **Teaching Studios and Classrooms**
   Areas inside teaching studios and classrooms on CityU campus, or the surrounding space in which IT services and resources are provided.
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. **IT Services**
   IT services include a range of services provided via the University's and related IT Service Providers' computers and communication networks, including for instance Email services, web hosting, data storage, resource booking, online library access, or online printing/copying.
6. **IT Services and Resources**
   IT Services and Resources include various IT services, manpower, information, data, and facilities to support the teaching, learning, research, and administrative activities at the University.
7. **IT Service Providers**
   IT Service Providers include various University departments and offices, including Central IT and their selected solution providers, that provide and manage IT Services and Resources.
8. **Email Services**
   The Central IT offers the following Email Services:
   a. Staff Email Services
      i. @cityu.edu.hk
      ii. @um.cityu.edu.hk
   b. Students Email Service
      i. @my.cityu.edu.hk
   c. Alumni Courtesy Email Service
      i. @my.cityu.edu.hk
   d. Retired Staff Courtesy Email Service for eligible staff
      i. @friends.cityu.edu.hk
   e. Specialised Emails (by application only)
      i. @gapps.cityu.edu.hk
9. **Obsolete Email Services**

The following email domains are no longer issued:

a. @mslive.cityu.edu.hk
b. @student.cityu.edu.hk
c. @alumni.cityu.edu.hk

G. Related Policies and Regulations

This document, the Policies on Use of IT Services and Resources, is only part of the University's set of policies and regulations governing IT use. The complete set includes also the following specific regulations:

1. Electronic Mail Regulations
2. Mass Communication and Social Computing Regulations
3. Campus Network Regulations
4. Electronic University Data Regulations
5. Teaching Studio and Classroom Regulations

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

H. Contact Information

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

(1) Electronic Mail Regulations

A. Purpose

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

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

B. Scope

All users of University provided *Email Services* are subject to regulations defined in this document. Specifically, courtesy email services users, including alumni and retired staff, are also subject to regulations defined in this document.

C. Statements

1. All emails sent from the 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 use email for the sole purposes of the operation of the University, save and except users of courtesy email services (such as "Alumni" and "Retired Staff").
3. The *Email Services* refers to a set of communications services and contents from the University. These include, but are not limited to, university announcements, service announcements, administrative messages, and CityU Newsletter. They are considered part of the services provided. Users will not be able to opt out from receiving them.
4. Eligible applicants may apply for "courtesy email service account". Conditions are also applied and subject to change by the University without prior notice.

The University shall have the right in its sole discretion to approve or refuse such application.

5. Users must inform the University of changes in their contact information. If the University has reasonable grounds to believe that the information has become untrue, inaccurate, or not current, the University has the right to suspend or terminate the *Email Services* and refuse any and all current or future use of the Services.
6. Email use for activities such as defamation, abuse, harassment, obscene acts, threats or other violations of legal rights (such as rights of privacy and publicity) of others is not allowed. Furthermore, the University's email address lists as well as other relevant contact information in the University's communications directories may contain personal data of the respective users and are for internal use only. These data may not be distributed to any external entity for mass mailing or used for any purposes other than those approved by the University.
7. 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.
8. 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.
9. The *Email Services* shall not be used for purposes that can reasonably be expected to cause, directly or indirectly, either excessive load on any IT services and resources or interference with others' use of such IT services and resources. Users shall also take all reasonable steps to avoid wastage of the IT services and resources provided, and the IT Service Providers reserve the right to levy charges on wasteful and / or inappropriate use of resources. For example, users must not send or forward chain email, unsolicited bulk email ("spam"), or excessively large email intended to block the recipient's mailbox.
10. To minimise spam, junk or otherwise harmful email, the University uses automatic email spam control system. This system automatically categorises incoming email based on the email services providers' algorithms. While any such system is adjusted from time to time by the email services provider, there is no way for Central IT to intervene in the system's algorithms.
11. To effectively and speedily stop the delivery of additional spam emails, *Central IT*, upon receipt of multiple complaints and review of them, may block ("blacklist") future delivery of such emails, even if they are not yet classified as spam by email service provider algorithms.
12. Users must not intentionally transmit any harmful computer programs, including computer viruses, worms, defects, trojans, or any other items of a destructive nature. Users shall also protect university computers in their possession to avoid unintended transmission of the above.

13. 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.
14. 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.
15. 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.
16. The *Email Services* must not be used as a storage mechanism for University records. Content/records should be stored and managed in appropriate systems such as document management systems, share drives, or other organized electronic filing systems. System backups for the *Email Services* are performed only for the purposes of disaster recovery, and for 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.
17. 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, a violation of the relevant IT Policies or Regulations or is otherwise objectionable in the sole discretion of Central IT.
18. The University or its delegate retains the right, at his/her own sole discretion, to create limits on the number of transmissions users may send or receive through the *Email Services* or the amount of storage space used at any time with or without prior notice.
19. 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.
20. Unsolicited massive emailing without explicit approval from the University, or broadcasting messages which are likely to harass or offend other users, or any communications which violate IT Policies and Regulations, or any other relevant laws and regulations are prohibited. Sending electronic messages to people you do not know or who do not need to receive the message is a nuisance.
21. Users intended to announce a message to large group of recipients are requested to use "CityU Announcement Portal (CAP)", the University's official

mass communication service. Sender must respect recipients' rights to optout from the mailing list by providing unsubscribing mechanism. Upon receipt of complaints about not fulfilling this requirement, the *Central IT* may at its discretion suspend the sender's email account and to remove the sent email from recipient's mailboxes without prior notifications. Details are set out in the "Mass Communication and Social Computing Regulations".

D. Enforcement

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

E. Terms and Definition

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

F. Related Policies and Regulations

This document, Electronic Mail Regulations, is only part of the policy. The "Policies on Use of IT Services and Resources" document contains a complete list of other relevant regulations.

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

G. Contact Information

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

(2) Mass Communication and Social Computing Regulations

A. Purpose

The acceptable use and unacceptable use of the *Email Services for mass communication*, and *publishing via personal web sites and social media platforms*, and related violation penalties, if any, are governed by the "Policies on Use of IT Services and Resources", "Electronic Mail Regulations", "Campus Network Regulations", "Electronic University Data Regulations", "Information Security Policies and Standards" and additional regulations defined in this document.

B. Scope

All users of university-provided *Mass Communication Services* (including email services, postings on CityU Announcement Portal; hosting webpages in University servers, subscribed services, with or without university domain or IP addresses; or any other CityU-provided electronic media such as digital signage); or postings to social media platform through CityU-provided IT services; or posting to social media platform in the capacity of CityU's employment stated explicitly or implicitly (collectively, "Service") are subject to regulations defined in this document.

C. Statement

1. CityU Announcement Portal (hereafter "CAP") is the University's official ecommunication service for both staff and students. CAP is setup to minimise emails overloading and provide a single pane of glass of all announcements made by university bodies, categorising for different personas.
    a. Users of email services should use "CityU Announcement Portal (CAP)" instead of emailing to large group of recipients. The University or its delegate may impose control on the number of emails to be sent by any individual.
    b. Depending on the settings of announcements made on CAP, the announcements may be shown on University website, daily email digests, campus digital signages, as well as mobile apps.
    c. Users must not use CAP to initiate a discussion or conversation, regardless of such discussion or conversation be carried out in or outside CityU provided IT Services and Resources.
2. Mass email senders should respect recipient's rights to opt-out from the mailing list. An opt-out or unsubscribe mechanism must be provided by the sender. Central IT will regularly check if mass email senders comply with the requirements above.
3. To help segregate various channels in the Service to their best use and to avoid information overloading, users should use only one of the channels to communicate the same/similar information to the same internal group.
4. Users should use the Service only to send or post materials that are legal, proper and in direct support of the vision, mission and role of the University.
5. Users must not use the Service for any illegal or unauthorized purpose.
6. Users are entirely responsible for all Content (including all data, text, information, links, images, multi-media data and other content) that published, posted, uploaded, distributed, disseminated or otherwise transmitted via the Service. The University shall not be liable or otherwise be

responsible for any claims of whatever nature relating to the Content, if the content posted are not duly authorised by appropriate authority from CityU.

7. Content posted will be public and stayed online for an infinite period of time and users should be fully aware of it.
8. Users should follow the terms of service of the related websites/platform.
9. Users should hold CityU harmless and indemnify CityU, and its delegate, subsidiaries, affiliates, officers, agents, employees, licensors, suppliers or partners, from and against any third party claim arising from or in any way related to their posting or publication of the Content through the Service, violation of regulations of the Service or any other actions connected with their use of the Service, including any liability or expense arising from all claims, losses, damages (actual and consequential), suits, judgments, litigation costs and attorneys' fees, of every kind and nature.
10. Users must not make personal attacks, defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others.
11. Users must not use the Service as for political appeals, editorializing, or partisan (including issue-partisan) lobbying.
12. Users must not post any inappropriate, defamatory, infringing, obscene, or illegal content.
13. Users should respect their audience, and shall not use defamatory and discriminatory terms, personal insults, ethnic slights, obscenity, or engage in any conduct that is not appropriate or acceptable to CityU. Users shall also respect the privacy of others, and shall not post the photos of individuals, named or not, on social media without their prior knowledge or permission.
14. Users must not post any Content that infringes any patent, trademark, copyright, trade secret or other proprietary right of any party (the "Rights"), or likely or intended to cause confusion that they are or connected with the owner of the Rights or are otherwise using the Rights with authorisation.
15. Users must not use the Service for commercial or profit-making activities, promotion of pyramid schemes, chainmail, etc.
16. Users must not download any file posted by another user that they know, or reasonably should know, that cannot be legally distributed in such manner.
17. If identifying themselves as a member of CityU on the social media:
    a. Users shall be aware of their association with CityU, ensuring their profiles and the content related are consistent with how they present themselves through CityU.
    b. It will be desirable for users to include a disclaimer in the profile section like this: “The postings I put up on this site are fully under my responsibility, and do not reflect the positions and views of CityU.”
18. 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 posted.

19. Users shall not provide sensitive, confidential or proprietary information of CityU, its staff, its students, its alumni or its units on the social media without authorization.
20. When making a reference, users should always link back to the source whenever possible.
21. Users must not restrict or inhibit any other user from using the IT Services and Resources.
22. Users must not remove, obscure or alter any copyright, trademark or other proprietary rights notices contained in or within the Service.
23. Users must not interfere with or disrupt the Service, servers or networks connected to the Service, or disobey any requirements, procedures, policies or regulations of networks connected to the Service.
24. Users must not use any robot, spider, site search/retrieval application, or other device to retrieve or index any portion of the Service or collect information about other users for any unauthorized purpose.
25. Users must not submit Content that falsely expresses or implies that such Content is sponsored or endorsed by the University or a third party.
26. Users must not promote or provide instructional information about illegal activities or promote physical harm or injury against the Service or individual.
27. Users must not transmit any viruses, worms, defects, trojan horses, or any items of a destructive nature.
28. It is fine to engage in lively and vigorous debates on social media, but users shall be mindful to be respectful to others and of their opinions. It shall be commendable for users to be the first to correct their own mistakes. Below are some standard etiquettes, or Do's and Don'ts for using the social media:
    a. Verify information before posting it.
    b. Make sure the links work.
    c. Be cautious when posting and tagging photos.
    d. Thank people for giving input or feedback, including negative ones.
    e. If friends/fans post postings that involve profanity, disrespectful comments, inaccurate or misleading information, etc., consider removing them. If postings are outright egregious, block the posters, or even report them to the social media if violence, pornography, smear, hate speech etc. are found.
29. Only use CityU logos or trademarks on the social media if users are authorized to do so.
30. The University or its delegate sees appropriate may modify or terminate the Service at any time with or without notice and users are bound by such changes.
31. If the University or its delegate is informed that any Content published through the Service does not appear to conform to the regulations, the

University or its delegate may investigate and may in good faith and in its sole discretion remove the Content. The University and its delegate have no liability or responsibility towards any person to carry out such investigation or remove such Content.

D. Enforcement

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

E. Terms and Definition

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

F. Related Policies and Regulations

This document, Mass Communication and Social Computing Regulations, is only part of the policy. The “Policies on Use of IT Services and Resources” document contains a complete list of other relevant regulations.

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

G. Contact Information

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

A. Purpose

(3) Campus Network Regulations

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

B. Scope

All users with access to the campus 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 Service Desk as soon as possible.
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 access points, 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*.
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*.

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

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

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

E. Terms and Definition

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

F. Related Policies and Regulations

This document, Campus Network Regulations, is only part of the policy. The “Policies on Use of IT Services and Resources” document contains a complete list of other relevant regulations.

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

G. Contact Information

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

(4) Electronic University Data Regulations

A. Purpose

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

B. Scope

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. In the event any electronic storage devices containing personal and / or sensitive data are lost, or users suspect there to be potential undesirable data leakage, users should report the incident to [the respective IT Service Provider(s)] in writing as soon as possible.
4. 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

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.

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

E. Terms and Definition

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

F. Related Policies and Regulations

This document, Electronic University Data Regulations, is only part of the policy. The “Policies on Use of IT Services and Resources” document contains a complete list of other relevant regulations.

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

G. Contact Information

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

(5) Teaching Studio and Classroom Regulations

The acceptable and unacceptable use of the facilities at the *Printing Areas, Teaching Studios and Classrooms* (collectively the Area) and related penalties, if any, are governed by the "Policies on Use of IT Services and Resources" and additional regulations defined in this document.

B. Scope

All users of the facilities at the *Printing Areas, Teaching Studios and Classrooms* 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 staff on duty.
2. The security guard or the staff on duty has the right to examine the activities, processes, or print outs to ensure that the users are observing the regulations.

A. Purpose

3. The Area is under video surveillance and the use and playback of the video footage is governed by the prevailing guidelines set out by the University.
4. A user at the Area must:
   4.1. use only the workstation he/she has booked through the Computer Reservation System;
   4.2. use only his/her own account to book the workstation and use the workstation only for academic work;
   4.3. follow the instructions in front of each laser printer and observe best practice/guidelines in related website when using the printing service;
   4.4. return to the Service Desk all loaned equipment or manuals 15 minutes before the service closing time;
   4.5. leave the Area immediately at its closing time, or at any other time when instructed to do so by the security guard or the staff on duty;
   4.6. 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 Area;
   4.7. practise green IT (e.g. printing hard copy only when absolutely necessary, powering off the workstation after use, etc.), and
   4.8. report any malfunction of equipment to the Service Desk for repair.
5. A user at the Area must not:
   5.1. cause any nuisance or disturbance to others (e.g. shouting, singing, playing music or computer game, etc.);
   5.2. install, alter, delete, or copy any software on computers;
   5.3. allow others to use his/her account(s) and CityU ID card;
   5.4. use any equipment for non-academic related work (e.g. printing blank paper, election materials, etc.);
   5.5. alter the location and connections of any equipment (e.g. power bar, network cable, monitor, keyboard, mouse, CCTV, etc.);
   5.6. connect any unauthorised devices to the network or AV equipment in the Area without prior approval;
   5.7. in any way deface or damage any equipment, manual, or other property;
   5.8. leave personal belongings unattended at any time;
   5.9. eat, drink, or play any form of game, and
   5.10. without prior approval from CSC, repair or attempt to repair CSC's equipment, or alter their hardware or software settings.

D. Enforcement

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

E. Terms and Definition

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

F. Related Policies and Regulations

This document, Teaching Studio and Classroom Regulations, is only part of the policy. The "Policies on Use of IT Services and Resources" document contains a complete list of other relevant regulations.

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

G. Contact Information

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