ISSC/2018-19/D02-A3

HONG KONG BAPTIST UNIVERSITY

GUIDELINES FOR USAGE OF INFORMATION RESOURCES

Date of issue: May 2019
For internal use only

TABLE OF CONTENTS

1. DOCUMENT CONTROL

1.1. Document status

Document name	Guidelines for Usage of Information Resources
Document code	ISSC/2018-19/D02-A3
Authored by	Information Security Sub-committee (ISSC)
Approved by	Information Technology Committee (ITC)
Version number	2.0
Date approved	June 2019

1.2. Revision history

Version number	Revision date	Summary of changes
1.0	July 2012	Initial version
2.0	May 2019	1) Restructure the document to establish a consistent format for the entire set of information security policies, standards and guidelines. 2) Add a new "Introduction" section to consolidate the original "Objective" and "Scope" sections. 3) Elaborate on the original "Policy statement" to form a new "Policy statements" section for setting out the overall security policy for usage of information resources. 4) Add a new "General guidelines" section for providing general guidance and security practices for users.

2.0 (Cont'd)	May 2019	5) Update "Acceptable usage" and "Restrictions" in various sections of information resources by referring to the latest security best practices and resolutions from previous meetings of the ISSC and ITC. 6) Add a new "References" section for relevant policies, standards and guidelines.

2. INTRODUCTION

2.1. Objective

The *Guidelines for Usage of Information Resources* (this document) is aimed at providing policy statements, together with guidance, concerning the position of Hong Kong Baptist University (HKBU) in relation to the use of information resources. It is also intended to assist all users in understanding their responsibilities and in exercising appropriate judgment when using the information resources.

2.2. Scope

Information resources refer to the assets which are used for creation, processing and storage of data or information in any form and any way. Such assets include, but are not limited to, the following:

- computer resources
- information systems and applications
- Internet/intranet
- email
- instant messaging
- portable storage
- anti-virus and anti-malware software
- network resources
- mobile computing devices
- remote access facilities
- copyright materials and software

3. POLICY STATEMENTS

3.1. Policy

3.1.1. Information security is everyone’s responsibility.

3.1.2. Users with access to HKBU’s information resources are responsible for protecting the data from unauthorised access, modification, duplication, destruction or disclosure, whether accidental or intentional.

3.1.3. Users are accountable and liable for all activities performed on information systems with their user accounts and should exercise all due diligence with respect to keeping their identity and login information safe and secure.

3.1.4. User accounts shall be uniquely assigned for access to HKBU’s information systems and applications.

3.1.5. All users shall observe and comply with the requirements set forth in this document. Requests for exception shall be submitted in writing to the Office of Information Technology (ITO) with appropriate justifications and mitigating measures.

3.1.6. Any inappropriate use of information resources or breach of any information security policies shall be reported to ITO and the Head of Department (HoD) concerned. When necessary, access to information systems or services shall be immediately suspended upon receipt of authorisation to do so.

4. GUIDELINES

4.1. General guidelines

4.1.1. Users shall use information legitimately and ethically. The following actions are strictly prohibited: acts of a malicious or nuisance nature, invasion of privacy, infringement of intellectual property rights, harassment, bullying, hacking, alteration of settings or data without authorisation, plagiarism, gaming, impersonation/identity theft, spoofing, gambling or any other unbecoming conduct.

4.1.2. When using the information resources, users shall comply with all applicable laws and regulations, such as:

- *Telecommunications Ordinance*
- *Crimes Ordinance*
- *Theft Ordinance*
- *Personal Data (Privacy) Ordinance*
- *Unsolicited Electronic Messages Ordinance*
- *Copyright Ordinance*

4.1.3. Users shall not use the information resources for activities that are unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane or that may constitute or encourage violation of any laws and regulations. These include activities:

- related to materials of a pornographic or obscene nature;
- promoting violence;
- constituting harassment or defamation to a third party;
- causing discrimination based on race, sex, religion, nationality, disability, sexual orientation, family status or age; and
- involving infringement of intellectual property rights.

4.1.4. Users shall use information resources primarily for teaching, learning, research, administrative support or providing social or community services.

4.1.5. Users shall not use information resources beyond their intended purposes, such as for:

- commercial or political purposes;
- personal gain, return or profit without proper authorisation; or
- unauthorised activities or access to any system or data.

4.2. Computer resources

Acceptable usage

4.2.1. When leaving a terminal, workstation, or other computing resources (such as a server room or a computer laboratory), users should, whenever applicable, log off their computing service in order that the relevant computing account will not be used by others.

4.2.2. Users shall follow safe computing practices such as never sharing their passwords, changing passwords regularly, logging out of systems at the end of a usage session, and protecting privacy as well as **sensitive information** (see Glossary (6.1) below) of the University.

4.2.3. Users must enable a password-protected screensaver (or equivalent software) on their desktops or laptops located in administrative offices (including the general office of academic departments and faculties/schools), student facilities and public areas, in order to protect information in the local storage and usage of IT resources through the network. The timeout or idle period to trigger a screensaver for desktops or laptops should not exceed 30 minutes.

4.2.4. Departments/offices should enable (or install) an appropriate screensaver on desktops or laptops located in their offices, student laboratories and common areas under their supervision.

4.2.5. Users should use only supported and updated operating systems and applications on their computing devices.

4.2.6. Users should ensure that their computing devices have been updated with the latest security patches.

4.2.7. Users should backup the data in their computing devices regularly.

4.2.8. Users should be cautious before opening any files or attachments and before clicking any hyperlinks on their computing devices.

<u>Restrictions</u>

4.2.9. Users must not develop programmes or make use of already existing programmes that harass other users, infiltrate a computer or computing system within or outside the University, damage or sabotage the hardware or software components of a computer or computing system, or gain unauthorised access to other facilities accessible via the network.

4.2.10. Users must not make excessive demands on the University's computing resources and capacity, e.g. by viewing streaming media not directly related to their job duties or educational needs, intentionally placing a programme in an endless loop, printing excessive amounts of paper, using peer-to-peer file-sharing programmes, or sending unauthorised chain letters or unsolicited mass mailings.

4.2.11. Users must not use the University's computing resources in a manner that may reasonably be expected to cause, directly or indirectly, unwarranted or unsolicited interference with the activities of other users.

4.2.12. Users shall not allow others to use their computing account to gain access to the University's computing resources.

4.2.13. Users must not let unauthorised persons use their computing devices.

4.3. Information systems and applications

<u>Acceptable usage</u>

4.3.1. Users must obtain proper authorisation before gaining access to the University's information systems and applications. Information systems and applications may be used only for the purposes intended and not for any other purposes (such as personal use, or unauthorised commercial or consulting work) unless specifically approved by the relevant University authority.

4.3.2. Departments/offices shall ensure workstations owned or under their management are compliant with the authentication on shared workstations policy; i.e. all workstations connected to the campus network should require proper authentication before access is granted to any user. If an authentication mechanism is not available, the identity of the user should be recorded.

4.3.3. Users' accounts for access to information systems and applications are for their own exclusive use, and they must not share their user accounts with others.

4.3.4. Users should take reasonable care to safeguard their Single Sign-On identity (SSOid) and any other system accounts, pay attention to ITO's security alerts and reminders to change their password, and set passwords according to the *User Account Password Policy*.

- An account password should consist of the following:
  - upper-case characters
  - lower-case characters
  - numbers
  - selected special characters (! - . ~ _ @)
- The password should be between 8 and 14 characters long;
- A password should expire after one year; and
- Reuse of previous passwords within one year is not allowed.

4.3.5. Users should use two-factor authentication whenever possible for central IT services, including but not limited to email and BUniPort, and other IT services accessible with the SSOid.

Restrictions

4.3.6. Users must not attempt to discover (i.e. obtain without approval) a password and should avoid allowing others to gain access to the information systems and applications designated for their own use.

4.3.7. Users must not attempt to circumvent or compromise security measures implemented within the University's information systems and applications or be engaged in any activity that may cause, purposely or otherwise, harm to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorised modifications to the University's data.

4.3.8. Users must not attempt to use the University's information systems and applications without authorisation or for purposes outside the intended ones.

4.3.9. Users must not use others' user accounts and passwords without authorisation.

4.4. Intranet and Internet

Acceptable usage

4.4.1. Users should access websites only for work and/or study. Accessing websites for any other purposes should be avoided, as such personal use will unavoidably increase the load on computing and information resources of the University, adversely affecting others who are using the resources for work and/or study.

4.4.2. Users should access the Internet and websites with due care against ransomware, malware infection, data leakage and other hazards.[1]

4.4.3. Users must ensure that information stored or published on the Internet (including documents in cloud drives, comments posted on social websites, blogs and discussion forums) does not involve any CONFIDENTIAL or RESTRICTED information of the University.[2]

4.4.4. At all times, downloading any software or applications from the Internet and installing them on the University's PCs without proper authorisation should be avoided, as such acts may compromise the security and integrity of the University computing environment.

[1] Please refer to *Data Leakage Prevention Policy* (ISSC/2017-18/D02), Hong Kong Baptist University, May 2018.

[2] Please refer to *Guidelines for Information Classification and Handling* (ISSC/2018-19/D02-A2), Hong Kong Baptist University, May 2019.

Restrictions

4.4.5. Users shall never publish, access or seek to access information in websites which may be considered unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane.

4.4.6. Users should not arbitrarily and unreasonably consume an inordinate amount of network bandwidth or system resources with media streams, graphics, data, etc.

4.4.7. Users must refrain from creating user accounts on Internet websites with names and/or passwords that are the same as those for their University's computing accounts.

4.5. Email

Acceptable usage

4.5.1. Sending emails that contain CONFIDENTIAL information of the University must be authorised by the respective information owner(s), and such emails must be encrypted before transmission and storage.[2]

4.5.2. All emails, including replies and forwarded emails, should contain the standard disclaimer statement of the University.

4.5.3. If a user's email signature contains his/her personal information, such as post title, office telephone number or mobile number, he/she should make sure those details are correct.

4.5.4. To delete an email message properly, it should be moved to the bin or trash folder of the user's email programme or account and then deleted from the bin or trash folder. Moving the email message to the user's own bin or trash folder will not automatically remove the email from their account, PC or laptop.

4.5.5. Users should check their emails regularly, delete unwanted messages and archive unnecessary messages that waste system resources and disk space.

Restrictions

4.5.6. Users should never send abusive emails or attachments, even if they are responding to an email of a similar nature. This includes e-mails targeting the recipient directly.

4.5.7. Users should never send emails, or include attachments in emails, the contents of which may be considered unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane.

4.6. Instant messaging

Acceptable usage

4.6.1. Users should exercise due care in avoiding malware infection or causing undue loading of the messaging service and University network when using the University's instant messaging facility.

Restrictions

4.6.2. Users should never send instant messages or send or receive file attachments via instant messaging if the content may be considered unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane.

4.6.3. Users should never send any instant messages or attach to these messages any University information that is classified as CONFIDENTIAL or RESTRICTED without proper encryption or authorisation.[2]

4.7. Portable storage

Portable storage refers to any removable electronic device or medium that has the capacity to store data, including but not limited to external hard drives, CDs and DVDs, floppy disks, tapes, smart or memory cards, USB drives, mobile phones, tablet PCs and laptops.

Acceptable usage

4.7.1. Users must ensure that all portable storage devices used to keep and/or process University information are protected by the same level of security as the information stored within them.

4.7.2. Only portable storage devices provided by the University should be used to store or transport University information, and the storage devices concerned should not be used for other purposes.

4.7.3. Storage of CONFIDENTIAL or RESTRICTED information in portable storage must be authorised by HoD.[2]

4.7.4. Storage of CONFIDENTIAL information in portable storage must be encrypted. Any transmission of encryption passwords or keys must be done through an alternative method (e.g. phone).[2]

4.7.5. **Care and storage**: Portable storage containing information related to the University should be secured in a place with locks or other access control devices. Important information stored on portable storage should be regularly backed up to an approved storage device (i.e. users' PC or designated file servers of the University).

4.7.6. **Cleansing and sanitisation**: Portable storage containing University information must be appropriately cleansed and sanitised after use. If non-rewritable portable storage devices or media, such as CDs and DVDs, are used, they must be destroyed by using a disintegrator grinding, smashing or burning.

4.7.7. **Disposal**: Users must ensure appropriate sanitisation of portable storage is performed before disposal. Portable storage devices that store CONFIDENTIAL or RESTRICTED information must be cleansed and sanitised (or destroyed) after use or before disposal.[3]

4.7.8. **Maintenance**: In case maintenance service is needed, users should backup and erase all data in portable storage before sending it to maintenance service providers.

[3] Please refer to Appendix A of *Guidelines for Information Classification and Handling* (ISSC/2018-19/D02-A2), Hong Kong Baptist University, May 2019 for proper sanitisation methods.

4.7.9. **Transmission**: Users must implement appropriate security measures when transporting portable storage.

4.7.10. **Loss or theft**: Users must report to the HoD and ITO as soon as possible if a portable storage device containing CONFIDENTIAL or RESTRICTED information is lost or stolen.[4]

Restrictions

4.7.11. Users must not keep University information on any private portable storage.

4.7.12. Users must not keep data related to personal matters on any portable storage provided by the University.

4.7.13. Users should never store data on any of the University's portable storage devices if the content may be considered unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane.

4.7.14. Portable storage devices containing CONFIDENTIAL or RESTRICTED information must never be connected to unknown/public workstations.

4.7.15. Users should never leave portable storage containing University information unattended at any time unless it is safely secured.

4.8. Anti-virus and anti-malware software

Acceptable usage

4.8.1. Users should stay alert against computer viruses and malware. Users should not attempt to copy, open, transfer to others or execute any piece of software or computer file that has been obtained from an unidentifiable source, e.g. via an email from an unknown sender or downloaded from a website hosted by unknown parties. On receipt of such dubious software or computer files, users should delete them immediately and permanently.

[4] Please refer to the incident management process as stipulated in the *Guidelines for Information Security Incident Handling* (ISSC/2017-18/D01), Hong Kong Baptist University, May 2018.

4.8.2. All computers and portable electronic devices that are to be connected to the University network, whether operated within or outside HKBU, should have anti-virus or anti-malware software installed and configured. This includes those to be used for accessing data from the University's web applications and information systems.[1]

4.8.3. The anti-virus or anti-malware software installed in computers with a physical connection to the campus network shall be managed and monitored by ITO's central endpoint management server for proper security control.

4.8.4. Anti-virus and anti-malware software shall be configured to receive regular updates on security patches and virus/malware signatures. Such updates must be carried out automatically at least once daily and without the need for manual intervention.

4.8.5. When available, the real-time scanning and protection features of anti-virus and anti-malicious software should be enabled for emails and local and network drives.

4.8.6. On-campus PCs and laptop computers connected to the University network should be scanned for computer viruses and malware regularly. Users should report any virus or malware infections to ITO as soon as practically feasible.

Restrictions

4.8.7. Users should not attempt to alter, disable or remove the anti-virus or anti-malware software installed on their PCs or notebook computers stationed at the University unless specifically approved by ITO.

4.8.8. Users should not attempt to interrupt or stop the course of a regular update of security patches and virus/malware signatures or scanning of viruses or malware in computers.

4.9. Network resources

Acceptable usage

4.9.1. Users should access the University network primarily for work-related or study-related purposes.

4.9.2. Incidental use of University's network services for personal matters is allowed, as long as such use is reasonable.

4.9.3. Users should make use of the official Wi-Fi access points (see Glossary (6.1) below) installed by ITO to connect their mobile devices to the campus network. The service set identifiers (see Glossary (6.1) below) of such access points have been published on the ITO website and are encrypted, with a lock icon or the word "secured" shown beside the SSOid.

Restrictions

4.9.4. Users must neither install any wireless router or access point on the University premises nor any device that may link any external network to the campus network, directly or indirectly by network routing, without authorisation from ITO.

4.9.5. Users shall never publish, access or seek to access information within the University network which may be considered unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane.

4.9.6. Users shall not share their account with anyone, use another user's account, even with permission, or allow the use of an established connection by anyone who is not an authorised member of the University.

4.10. Mobile computing devices

Mobile computing devices refer to any portable computing and communication equipment with the capability to process and store information, including but not limited to smartphones, tablet PCs, and laptops.

Acceptable usage

4.10.1. Users must ensure that effective security measures are in place to protect the mobile computing devices that store or process sensitive information of the University against unauthorised access.

4.10.2. Users should protect and safeguard their mobile computing devices with due care. When not in use, the devices should be screen-locked. Users should never leave them unattended any time.

4.10.3. Storage or processing of CONFIDENTIAL or RESTRICTED information in mobile computing devices must be approved by the HoD.[2]

4.10.4. Users should store only the minimum amount of University information on a mobile computing device for the shortest possible time required. CONFIDENTIAL information stored on mobile computing devices must be encrypted.

4.10.5. Users should use the following security measures wherever possible to protect the information from being accessed by unauthorised parties:

- password protection for accessing the mobile computing devices;
- time-out protection (e.g. password-protected screensavers, screen or keyboard locks); and
- encryption for sensitive information, e.g. CONFIDENTIAL information or personal data.

4.10.6. Users should report immediately to the HoD and ITO about the loss or theft of mobile computing devices containing CONFIDENTIAL or RESTRICTED information. They should follow the formal incident management process in accordance with the *Guidelines for Information Security Incident Handling* (ISSC/2017-18/D01), Hong Kong Baptist University, May 2018.

4.10.7. Mobile computing devices not provided by ITO, including personally owned devices and devices provided by departments, are considered bring-your-own-devices (BYOD). Users should comply with the guidelines as stipulated in *Bring-Your-Own-Device (BYOD) Policy* (ISSC/2017-18/D03), Hong Kong Baptist University, May 2018.

Restrictions

4.10.8. Personal mobile computing devices are not allowed to be used for handling University information unless such information is intended for public consumption or prior approval from the relevant University authority is obtained.[2]

4.10.9. Users should never handle information using the University's mobile computing devices if the content may be considered unlawful, harmful, threatening, libellous, defamatory, obscene, scandalous, inflammatory, pornographic, indecent or profane.

4.10.10. Users should not download or install mobile apps or software from unknown sources.

4.10.11. Users must not connect the University's mobile computing devices to any unknown or unsecure wired or wireless network.

4.10.12. Users must not leave mobile computing devices unattended.

4.10.13. Users should not open SMS, instant messages or emails from unknown senders. Suspicious messages or files may contain malicious content and should be removed from the University's mobile computing devices immediately.

4.10.14. Users should never activate ad hoc data transmission functions, such as infrared or Bluetooth, unless it is absolutely necessary for legitimate work or educational purposes and the transmission takes place between trusted parties.

4.10.15. Users must not share the University's Wi-Fi connection with non-HKBU personnel. On University premises, users should not enable Wi-Fi personal hotspots, as they may interfere with the University's standard Wi-Fi access points.

4.11. Remote access facilities

Acceptable usage

4.11.1. Users must use the University's Virtual Private Network (VPN) only for legitimate work or educational purposes.[5]

[5] Please refer to *Remote Access Security Standard* (ISSC 2018-19/D01-A3), Hong Kong Baptist University, November 2018.

4.11.2. Users should avoid connecting to unsecured Wi-Fi or Bluetooth networks when using the University's VPN or accessing the University's data or systems remotely.

4.11.3. Users should ensure their personal computing devices used to connect to the University network meet the security requirements of the University-owned equipment for remote access.

Restrictions

4.11.4. Users should never provide their remote access login credentials to any outside parties. Remote access for external parties is permitted only when:

- it is required for the external parties to deliver agreed services to the University;
- the remote access login credential is granted and authorised by the appropriate University authority in accordance with the *Remote Access Security Standard* (ISSC/2018-19/D01-A3), Hong Kong Baptist University, November 2018.

4.11.5. The responsible department/unit should advise ITO to revoke the remote access login credential immediately upon the completion or termination of the agreed services with the external parties.

4.11.6. Users must not attempt to remotely connect to the University network or information systems from any hosts with insufficient security protections or through unsecure external networks.

4.12. Copyright materials or software

Acceptable usage

4.12.1. Any use of copyright materials or software within the University must be properly licensed and any terms and conditions set out in licence agreements must be fully complied with.

4.12.2. Users should take reasonable care to observe the provisions under the *Copyright Ordinance* when using the University's IT resources, by, e.g.:

- downloading copyright protected materials or software from the Internet or intranet;
- installing or running copyright software;
- copying software for use in University's PCs or laptops; and
- using file-sharing technology, such as peer-to-peer programmes to download copyright materials or software.

4.12.3. Users must remove or uninstall any copyright materials or software that are in violation of the respective licensing agreements.

4.12.4. ITO and the relevant departments must keep adequate records of any copyright materials and software to ensure the licensing conditions are adhered to at all times.

Restrictions

4.12.5. The University does not authorise or condone any infringement of the copyright law. Users who fail to observe the rules are personally liable for any consequences. Furthermore, disciplinary action in accordance with the University's policies and regulations may be instituted against offenders.

4.12.6. Users must not make or use illegal copies of copyright materials or software, store or install such copies within the University systems, or transmit them over the University network. This includes infringing materials transferred via peer-to-peer networks and materials illegally copied from other media. The University reserves the right to remove infringing materials or materials which are likely to be infringing from the University's IT systems and networks to block the transfer of such materials by email or other means.

4.12.7. Users must not in any way modify or alter the content of copyright materials or software within either the University's computing environment or the University's information systems.

5. REFERENCES

5.1. Policies, standards and guidelines

(a) *Bring-Your-Own-Device (BYOD) Policy* (ISSC/2017-18/D03), Hong Kong Baptist University, May 2018.

(b) *Cloud Service Policy* (ISSC-2016-17-D04), Hong Kong Baptist University, May 2017.

(c) *Code of Practice on the Personal Data (Privacy) Ordinance,* Hong Kong Baptist University, May 2019.

(d) *Data Leakage Prevention Policy* (ISSC/2017-18/D02), Hong Kong Baptist University, May 2018.

(e) *Guidelines for Information Classification and Handling* (ISSC/2018-19/D02-A2), Hong Kong Baptist University, May 2019.

(f) *Guidelines for Information Security Incident Handling* (ISSC/2017-18/D01), Hong Kong Baptist University, May 2018.

(g) *Remote Access Security Standard* (ISSC/2018-19/D01-A3), Hong Kong Baptist University, November 2018.

(h) *User Account Password Policy* (ITO/IFS/P002/2018), Hong Kong Baptist University, December 2018.

6. APPENDIX

6.1. Glossary

(a)	Access point	A device that creates a wireless local area network, usually in an office or large building.
(b)	Sensitive information	Either “Confidential” or “Restricted” data or information as defined in *Guidelines for Information Classification and Handling* (ISSC-2018-19-D02-A2), Hong Kong Baptist University, May 2019; or Personal data as defined in *Code of Practice on the Personal Data (Privacy) Ordinance*, Hong Kong Baptist University, May 2019.
(c)	Service set identifier	Service set identifier is a name assigned to a Wi-Fi network for users to identify and make connections to it.