THE HONG KONG POLYTECHNIC UNIVERSITY
香港理工大學

Acceptable Use Policy

for

University Information Technology Facilities and Services

[P-2]

VERSION 3.0

Contents

1 Document Control

1.1 Document Status

Document Name	Acceptable Use Policy of University Information Technology Facilities and Services
Document Code	P-2
Author	Information Technology Services Office
Version Number	3.0
Document Status	Approved
Date Approved	June 2018
Date of Next Review	September 2020
Superseded Version	2.0

1.2 Document History

Version Number	Revision Date	Summary of Changes	Authored By	Approved By
3.0	2018	In response to the promulgation of the University Data Governance Framework, the following sections are updated: • 3.1 Definition • 4.2 Business Purposes and Other Uses • 4.6 Monitoring of University IT Resources • 4.7 Information Security and Data Privacy	ITS	DoIT
2.0	2015	Re-organization of the Policy structure and content update	ITS	DoIT
1.0	2002	Document Creation	ITS	DoIT

2 Introduction

2.1 Purpose

The purpose of this "Acceptable Use Policy of the University Information Technology Facilities and Services" (Policy) is to ensure that all use of the **University Information Technology (IT) Resources** is legal, ethical, safe and consistent with the aims, values and objectives of the University.

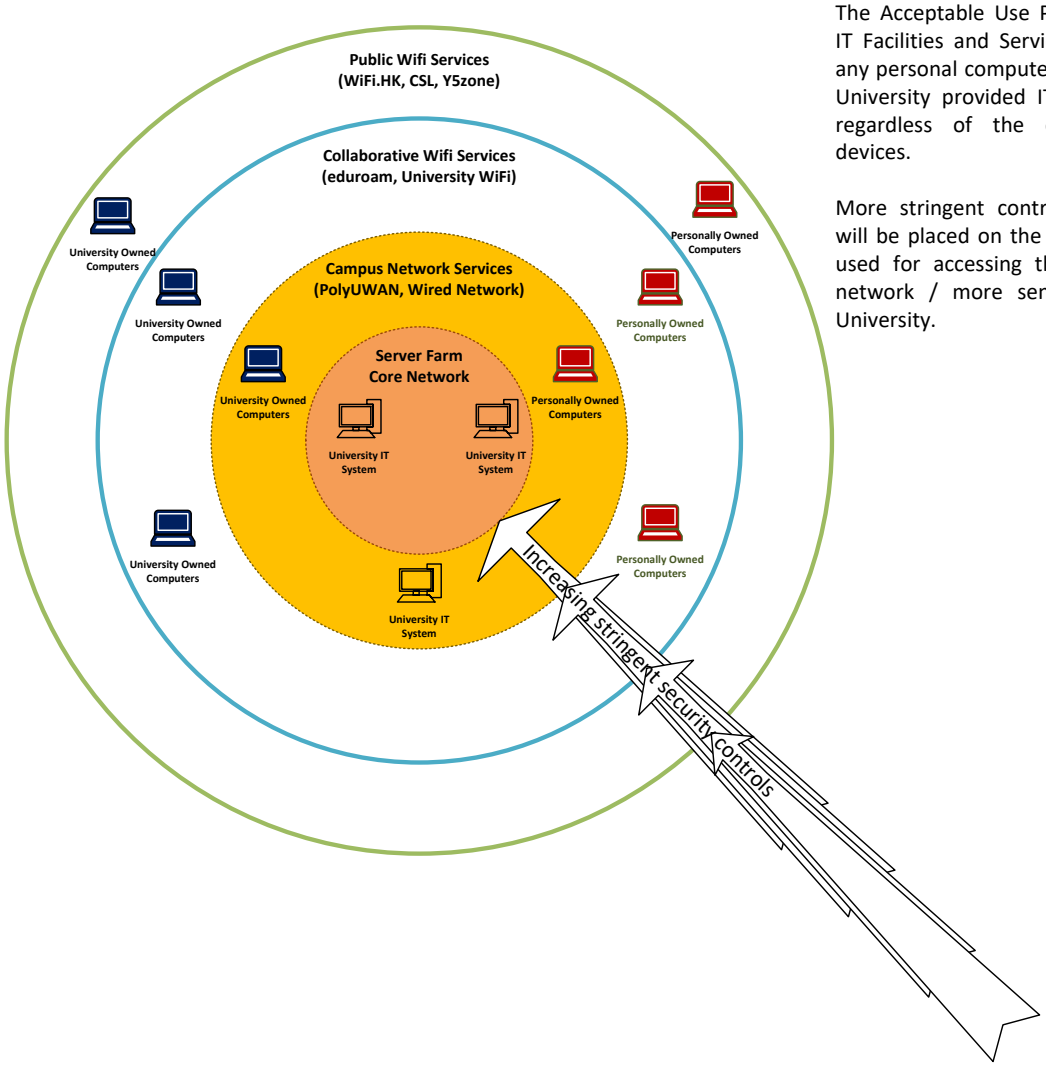
2.2 Scope

This Policy governs all uses of University IT Resources regardless of equipment ownership or administration; whether the use is direct or indirect.

This Policy applies to all **Users of the University IT Resources** (Users) whether affiliated with the University or not and to all use of these resources from on-campus or in remote locations. This Policy applies to all users of equipment owned or administered by the Information Technology Services Office (ITS); individual departments or by individuals which are connected to University IT Resources.

Connection by personally owned equipment to University IT Resources requires adherence to this Policy.

The following diagram illustrates the scope of applicability of this Policy:



The Acceptable Use Policy for University IT Facilities and Services is applicable to any personal computers connected to the University provided IT network services, regardless of the ownership of the devices.

More stringent controls / requirements will be placed on the devices as they are used for accessing the inner University network / more sensitive data of the University.

2.3 Structure of this Policy

This Policy consists of two sections which are "Core Policy Statements" and "IT Service Specific Policy". The "Core Policy Statement" section depicts the acceptable use policy statements which are applicable to the use of all University IT Resources. "IT Service Specific Policy" sections are enclosed in the **Appendix II** of this document which depicts the policy statements applicable to specific IT facilities and services.

3 Definitions and Conventions

3.1 Definitions

The following are the definition of the terms used in this Policy.

Term	Definition
Campus Network	"**Campus Network**" is set of interconnected local area networks serving the University.
HARNET	"**HARNET**" is the wide area network which links up the campus networks of the eight tertiary institutions in Hong Kong.
NetID	The PolyU NetID (Network IDentity) is a unique personal identifier for Users to access the central IT facilities and services.
Personal Data	"**Personal Data**" is defined under the Personal Data (Privacy) Ordinance to mean any data: • Relating directly or indirectly to a living individual; • Form which it is practicable for the identity of the individual to be directly or indirectly ascertained; and • In a form in which access to or processing of the data is practicable.
Data Classification Scheme	Data of the University are classified into four categories, namely "Restricted", "Confidential", "Internal Use" and "Public". For details about the data classification definition, please refers to the Data Governance Framework at: https://www2.polyu.edu.hk/DAG/Data%20Governance%20Framework.pdf
Staff	"**Staff**" are people employed by the PolyU irrespective of the employment period and terms.
Third Party Suppliers	"**Third Party Suppliers**" are all external parties that provide service to the University in respect of information systems and business activities.
User(s)	"**Users**" are the personnel, including staff members, students and third party suppliers, who have access to the University's information systems or information.
University Information Technology (IT) Resources	University IT Resources are the IT facilities and services that the University provided to Users for supporting their academic, administrative, commercial

	and community activities of the University. The list of University IT facilities and services under the governance of this Policy could be found at ITS Website: https://www.polyu.edu.hk/its/service-catalogue/all-services

3.2 Conventions

The following is a list of conventions used in this document:

- **Shall** - the use of the word 'shall' indicates a mandatory requirement.
- **Should** - the use of the word 'should' indicates a requirement for good practice, which should be implemented whenever possible.
- **May** - the use of the word 'may' indicates a desirable requirement.

3.3 Responsibility

The University shall ensure that Users are aware of this Policy by:

- Providing access to a copy of this Policy;
- Reminding Users of the need for compliance with this Policy; and
- Providing updates of this Policy as needed.

Users shall abide by this Policy while using University IT Resources.

4 Core Policy Statements

The "Core Policy Statement" section covers acceptable use policy statements which are applicable to the use of all University IT Resources.

4.1 Adherence to Laws, Regulations and Policies

Users shall be aware that the use of these resources is subject to the Laws and Regulations of the Government of Hong Kong Special Administrative Region, and the Policies of the University. This includes but is not limited to copyright, intellectual property, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, civil and criminal laws.

University IT Resources shall not be used in any manner contrary to the law or likely to contravene the law. The University is required to report contraventions of the law and suspected offenders to the law enforcement authorities.

4.2 Business Purposes and Other Uses

University IT Resources are primarily provided to Users for supporting the academic, administrative, commercial and community activities of the University. All electronic files, documents and email messages that are created and stored on the University IT Resources are considered as University data which are subject to review by authorized personnel of the University.

Users may use the University IT Resources for personal use provided that the use is not excessive and does not breach this Policy. Personal use of the University IT Resources, except for students enrolled at the University, should be incidental and kept to a minimum. The electronic files, documents and email messages created during the personal use of University IT Resources shall not be kept on the University IT facilities. For example, use of such resources by a staff member for other than work-related matters should be reasonable and limited so that it does not prevent the staff member from attending to and completing work effectively and efficiently, does not incur additional cost to the University, and does not preclude others with work-related needs from using the resources, including the shared campus and Internet bandwidth. Individual departments or units may place additional restrictions on personal use of the resources by their staff members.

4.3 Offensive or Inappropriate Material

University IT Resources shall not be used for purposes that are defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including but not limited to content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

Users who receive unsolicited offensive or inappropriate material electronically should report it to their immediate supervisor, Head of Department or to the Office of the Director of Information Technology, as appropriate.

4.4 Copyright Infringement

Users shall comply with the prevailing copyright laws and requirements regarding the use and distribution of copyright protected materials including but not limited to software and audio/visual recording. Users who infringe the copyright laws may be subject to criminal and civil proceedings.

Users shall ensure that the software and data they install and use are legal and properly licensed, and the terms and conditions of the license are not violated. In particular, users should note:

Users should not copy the software from the campus network and install it into other machines without obtaining appropriate licenses. Unauthorised copying and distribution of software is prohibited.

4.5 Defamation

University IT Resources shall not be used for disseminating material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or the University liability.

4.6 Monitoring of University IT Resources

Users shall be aware that the use of University IT Resources may be monitored for detecting the following anomalies:

- Abnormal CPU utilization and active processes on IT systems;
- Licensed software violations;
- Sudden surge in network utilization and errors;
- System and security log anomalies; and
- Abnormal user account activities on University IT systems and campus network;

System and network activity log information is generated from IT computing devices and collected to a centralized security information and event management systems under ITS' management.

The log information generated during monitoring process may also be used for the following purposes:

- Policing regulatory compliance
- Detecting and investigating crime or unauthorized use
- Safeguarding the integrity of the University's Information Technology Infrastructure
- Capacity planning for network expansion and service upgrades
- Institutional planning
- Enhancement of teaching and learning experience
- Statistical analysis, academic researches, quality assurance and review

Only the personnel who are authorized by the Director of Information Technology shall access the collected information through the monitoring process. The authorized personnel shall:

- respect the privacy of others;
- handle the log information in observance with the guidelines and privacy policy statement published by the University;
- not examine any user related information unless the equipment is subject to an authorized forensic examination or with the permission of the user in concerned;
- not use or disclose information realized in the monitoring process for purposes other than those for which the process was approved;
- safeguard information collected in the monitoring process; and
- destroy information collected in the monitoring process when it is no longer required.

It shall be considered a disciplinary offence for anyone to engage in monitoring activities without formal authorization from the Director of Information Technology.

4.7 Information Security and Data Privacy

The University recognises the importance of information security and is committed to ensure all business activities performed using University IT Resources are protected and maintained. Users shall comply with the University Baseline Information Security Policy while using the University IT Resources.

A user account, namely NetID, is uniquely assigned to individual User for access to the University IT Resources. Users are accountable and liable for all activities performed on University IT Resources with their NetIDs and shall exercise all due diligence with respect to keeping their NetID and NetPassword safe and secure. Users shall not disclose or share their user account information with another person. Users shall regularly change their passwords and immediately report to ITS Help Centre if their user accounts are known or suspected to have been compromised in any way.

Users with access to University information are responsible for protecting the information from unauthorized access, modification, duplication, destruction, or disclosure whether accidental or intentional. Users shall handle Personal Data with due care in accordance with the relevant University policies and guidelines.

Users shall refrain from any action that interferes with the supervisory, accounting and monitoring functions of the systems or from any action that is likely to have such an effect. Users shall refrain from creating and/or implementing code intended, even periodically, to interrupt or interfere with networked systems or services. Users shall refrain from knowingly propagating computer viruses or presumed computer viruses. Users shall not conduct unauthorized port scans and initiate nuisance or denial-of-service attacks, nor respond to these in kind.

4.8 Service Termination and Policy Violation

The University may block, suspend, or terminate the use of the IT Resources at any time for any reasons. Reasons for the University taking such action includes, but is not limited to, the following:

a. Users' breaching this agreement; or
b. User authentication information which cannot be verified or validated;; or
c. Users' actions that the University believes could cause financial loss or legal liability to the University or other users of the IT service; or
d. Use of IT services in a manner that violates the law or the University's policies; or
e. Use of Information systems that poses security threats to other information systems of the University; or
f. Necessary routine network maintenance work affecting all Users.

Any breach of this Policy shall be reported to the Director of Information Technology and the Head of the Department concerned and/or the University's disciplinary authority for appropriate actions.

The Director of Information Technology may appoint an investigator to examine information stored in or transmitted by implicated University Information Systems in accordance with the Personal Data (Privacy) Ordinance. The implicated IT Resources may be secured by the University while the suspected breach is being investigated.

~~~~~~End of Core Document~~~~~
~~~~~~

Appendix I: List of University IT Resources

The Acceptable Use Policy of University IT Resources governs the use of all IT facilities and services connected to the University network, whether owned or administered by the Information Technology Services Office or by individual departments, or by individual staff members.

The list of University IT Services provided by the Information Technology Services Office could be found at:

https://www.polyu.edu.hk/its/service-catalogue/all-services

Appendix II: IT Service Specific Policy

Some service specific acceptable use policies also apply. These service specific acceptable use policies are in addition to the general acceptable use policies defined in the previous section:

1. Desktop Management Service
2. Email, Messaging and Collaboration Services
3. PolyU Student Hall Network
4. NetID Management Service
5. Network Access Services
6. Student Computer Centre (SCC)

A 2.1 Acceptable Use Policy for Digital Workspace Management

In addition to the Acceptable Use Policy for University IT Facilities and Services, this policy defines the regulations for the use of personal computers including the University provided personal computers, Macintoshes, workstations, portable computers, handheld computers, personal digital assistants, and similar computers dedicated to a single user's activity. Violation of this policy may result in suspension of the use of the equipment or access to University IT resources.

1. Security Requirements on Personal Computers Connected to the University Campus Network

- The University Baseline Information Security Policy constitutes the minimum information security requirements that shall be observed and followed by all those with access to the University Information Systems, including Staff members, students, visitors and Third Party Suppliers. These security requirements apply to any Personal Computers connected to the University Campus Network including University Provided Personal Computers.

- All Personal Computers connected to the University Campus Network including University Provided Personal Computers shall be protected with anti-malware solutions running the latest virus scanning engines and signatures. Users shall ensure these anti-malware solutions are running properly on their workstations. If in doubt, Users shall contact ITS Help Centre for assistance.

- All Personal Computers attached to the University network, including University Provided Personal Computers shall utilise the latest security patches where possible.

2. Workspace Management and the Enterprise Active Directory Service

- All Personal Computers connected to the University Campus Network shall be registered in the University Enterprise Active Directory, if possible, in order to ensure the highest level of safety and security. In particular, User departments shall ensure that all University Provided Personal Computers running a Microsoft Windows Operating System or an operating system that interoperates with Windows Active Directory Domain and that are connecting to the University Campus Network are connected and managed through the Enterprise Active Directory.

- University policies and other actions, with regard to security hardening settings, patch levels or operating parameters, shall be applied and implemented on computers that have joined the domain.

- Where a business reason exists for a Personal Computer which is connected to the University Campus Network, not to be connected to the University Enterprise Active Directory, an exception request may be constructed by the departmental Computer Liaison Officer, endorsed by the Head of Department and approved by Director of Information Technology. User departments shall be responsible for applying the appropriate University security protections on these non-AD managed computers to ensure these personal computers are secure and not used for attacking other systems.

- All Personal Computers connected to the University Campus Network shall comply with a set of standardized security hardening configurations. In particular, Users of University Provided Personal Computers shall not alter these settings without the consent of the Information Technology Services Office. Exception requests based on business justifications, may be constructed through the departmental Computing Liaison Officer, endorsed by the Head of Department and approved by Director of Information Technology.

- All the University Provided Personal Computers shall be assigned with a unique machine identifier, i.e. hostname, in accordance with the University defined computer naming convention standard. Users shall not alter the hostname of their workstations without the consent of the Information Technology Services Office.

3. Least Privilege Policy

- Users shall be granted the minimal level of access and privilege necessary to perform their roles and duties. Where Users require a variation from this least privilege access policy they may apply for an exception based on business justifications endorsed by the Head of Department concerned.

4. Licensed Software

- Users shall not use unlicensed software on Personal Computers connected to the University Campus Network.

5. Remote Access and Assistance

- IT Support Staff may use remote assistance support software to support a User's machine but only with the explicit authorisation of the User and in their presence.

- All remote administrative and technical tasks connecting to the University Campus Network shall be conducted via the central Virtual Private Network service.

6. IT Security Incident Reporting and Response

- All Users shall report any security breaches to ITS Help Centre as quickly as possible to limit the impact of the security incidents to the University.

- The University shall take all necessary actions to protect the Campus Network as a whole, including temporary disconnection or suspension of implicated devices, compromised systems or user accounts in the event of a security incident.

- Any breach of security shall be reported to the Director of Information Technology and the Head of the Department concerned and/or the University's disciplinary authority for appropriate actions. Immediate suspension of access to University's IT facilities and services may be a necessary consequence of a security breach.

A 2.2 Acceptable Use Policy for Email, Messaging and Collaboration Services

E-mail is an official communication channel among staff and students at PolyU. Proper use of e-mail and other electronic communication mechanisms will avoid waste of resources and enable proper communication with target recipients.

Users should not use University electronic communication services for the following purposes:

- conducting commercial functions, such as marketing or business transactions
- sending irrelevant or chain mails to a large number of recipients
- broadcasting messages which are likely to harass or offend other users
- any communication which violates applicable laws and regulations

Users should also observe that proper and courteous language should be used in communications, and sending communications in the name of another person and/or anonymous communication is unacceptable. The University's e-mail address lists are for internal use and may not be distributed to external entities for purpose of mass mailing.

Please find more details on policies and guidelines on the use of e-mail and other electronic communications at:

https://www2.polyu.edu.hk/PolyU/General_Notices/PolyU_EMessaging_Usage_Policy.pdf

A 2.3 Acceptable Use Policy for PolyU Student Hall Network

The Hong Kong Polytechnic University student hall network is an extension of the University's campus network. The hall network, which is TCP/IP based, facilitates hostel users to access services such as e-mail, file transfer and Internet surfing.

The hall network, like the overall campus network, is provided and administered by ITS. Use of the hall network is governed by the rules and regulations of the campus network as well as those specific to the hall network, as stipulated, updated and promulgated from time to time by the University. Please find details of "Regulations Governing the Hall Network" at:

http://www.polyu.edu.hk/its/policies-and-standards/51-policies-and-standards/200-hall-network.

A 2.4 Acceptable Use Policy for NetID Management Service

PolyU NetID is the user's personal identification and access key to all University managed IT services. Activation of the NetID by the user implies the user's acceptance of the University's Acceptable Use Policy for IT facilities and services.

The NetID owner is responsible for maintaining and safeguarding the confidentiality of the NetID, and is responsible for all activities that occur under the NetID account, and hence any consequence that may result from its use.

The NetID and associated password constitute an individual's electronic identity and the User must safeguard it vigourously or risk identity theft.

The NetID owner should not disclose or share the account with another person. Users should regularly change their passwords and immediately report to the ITS Help Centre if the NetID or NetPassword is known or suspected to have been compromised in any way.

Policies Specific to the Use of the NetIDs can be found at:

http://www.polyu.edu.hk/its/pusecure/policy.php

A 2.5 Acceptable Use Policy Specific to Network Access Services

The PolyU campus network is a member of the HARNET network. In additional to the Acceptable Use Policy for the University IT Resources, all Users are required to observe the "HARNET Acceptable Use Policy". Please find details of "HARNET Acceptable Use Policy" at URL: http://www.jucc.edu.hk/haup/

A 2.6 Policies Specific for the Use of the Student Computer Centre (SCC)

PolyU students and staff with valid PolyU Student/Staff ID cards can use the SCC computing facilities on a first-come-first-served basis. Connection of any device or installation of software other than those installed by SCC is prohibited. Alteration, deletion or copying of any licensed software from SCC is strictly forbidden and may be illegal. Printing and scanning of material at SCC must comply with the copyright law.

Please find details of the rules and regulations of the Student Computer Centre at:

http://www.polyu.edu.hk/its/policies-and-standards/51-policies-and-standards/201-rules-for-student-computer-centre-users

~~~~~~End of Document~~~~~
~~~~~~