Information Communication Technology Acceptable Usage Policy

Intent

James Cook University Singapore seeks to provide it's Authorised Users with secure and timely access to Information Communication Technology (ICT) Services to facilitate learning and teaching, research and innovation, engagement and other functions of the University.

This Policy is intended to:

- provide a clear statement of responsibilities for all Authorised Users of University ICT Services, including what constitutes acceptable and unacceptable use;
- outline the provision, modification and removal of access to University ICT Services; and
- express the commitment of the University to maintaining secure, effective and reliable University ICT Services.

Scope

1. This Policy applies to all Authorised Users of the University ICT Services managed by the University or third party providers on behalf of the University, both on and off campus.
2. University ICT Services are the property of the University. Anything sent or received using the network, systems and facilities of the University will therefore be transmitted and stored on University property (or on third party property on behalf of the University).

Definitions

Authorised User - a person who has been provided with an Authentication Credential by the University to access University ICT Services. Various categories of users are documented in the ICT Acceptable Use Procedures.

Authentication Credential – user identification and password, username and passcode, PINs or other secret means used to gain access to University ICT Services.

Personal Information - information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

University ICT Services - facilities and services provided to an authorised user including software, communication devices and computing infrastructure under the control of the University (or a third-party provider on the University's behalf) that provides access to information in online or electronic format.

Policy

1. Acceptable Use of University ICT Services

1.1 This Policy reinforces the provision of a fair, safe and productive computing environment for the University community, by establishing clear responsibilities for Authorised Users that do not adversely impact the University's operations, assets or reputation.

1.2 All Authorised Users must act in accordance with this Policy and all other applicable University policies and procedures (including, without limitation, the ICT Acceptable Use Procedures).

1.3 University ICT Services covers Republic of Singapore legal jurisdictions. Authorised Users have a personal responsibility to be aware of the jurisdiction that applies when using University ICT Services.

1.4 Subject to Clause 1.5, Authorised Users are permitted to use University ICT Services for properly authorised and supervised business, education or research purposes, providing that the use:

a. is lawful;
b. is in a responsible, ethical and equitable manner;
c. is consistent with the values of the University as outlined in the University's codes of conduct;
d. does not create an intimidating or hostile work or study environment for others;
e. does not jeopardize the provision of a fair, safe and productive computing environment; and
f. does not adversely impact the University's operations, assets or reputation.

Authorised Users who are unsure whether a proposed use is permitted or authorised should seek written approval from their supervising head of organisational unit (eg. Dean or Director).

1.5 University ICT Services must not be used in any manner, which the University considers to be inappropriate, this may include, but is not limited to:

a. accessing pornography;
b. unauthorised monitoring of electronic communications;
c. knowingly downloading, storing, distributing or viewing of offensive, obscene, indecent, or menacing material. This could include, but is not limited to, defamatory material, material that could constitute racial or religious vilification, discriminatory material, material that incorporates gratuitous violence or frequent and highlighted bad language;
d. stalking, blackmailing or engaging in otherwise threatening behaviour;
e. any use which breaches a law, including copyright breaches, fraudulent activity, computer crimes and other computer offences;
f. transmitting spam or other unsolicited communications; or
g. the introduction or distribution of security threats, including a virus or other harmful malware.

1.6 Limited personal use of University ICT Services is acceptable, providing that that use is otherwise in accordance with this Policy. Limited personal use of University ICT Services is a privilege.

1.7 Authorised Users must not attempt to gain unauthorised access to University ICT Services (and the information stored thereon) to which they have not been given access or permit others to do so.

1.8 Authorised Users must not tamper with University ICT Services that may potentially cause performance degradation, service instability, or compromise operational efficiency, security or fair use.

2. Authorised Access and Restriction

2.1 All Authorised Users are permitted to access the University ICT Services, at a level commensurate with their position, role, delegated authority or student status.

2.2 In accordance with the ICT Access and Account Management Procedures, access to all University ICT Services will be removed when the relationship between Authorised Users and the University ceases.

2.3 Authorised Users must not use their access to University ICT Services to gain inappropriate personal, academic, financial or other advantage.

2.4 Authorised Users must maintain the confidentiality of any Personal Information accessed via University ICT Services.

2.5 Authorised Users of University ICT Services are not permitted to provide others with their Authentication Credential(s). It is the responsibility of Authorised Users to ensure that their Authentication Credentials are securely stored as they are responsible for all activity initiated from their account or with their Authentication Credential(s).

3. Software Licenses

3.1 Software purchased by the University is licensed primarily to the University, however approval may be granted to Authorised Users for use at home or other locations on non-University owned computers during the course of work or study with the University in accordance with the ICT Acceptable Use Procedures.

3.2 Authorised Users must comply with contractual obligations and terms and conditions of use stated in the software license agreements entered into by the University.

3.3 Authorised Users must discontinue use and un-install the software from non-University owned computer(s) upon cessation or termination of employment or completion of study, or upon notification by the University of its termination of the software license agreement.

4. Monitoring and Privacy

4.1 The University reserves the right to monitor, access, log and analyse the activities of Authorised Users, and of University ICT Services, and conduct reviews and audits as necessary.

4.2 The University reserves the right to block or filter any use that breaches this Policy or exceeds the University's acceptable level of risk.

4.3 Subject to the provisions of the University's Information Privacy Policy and relevant legislation, the University may disclose the contents of electronic communications without permission of the Authorised User.

4.4 The University may take any action deemed necessary to remedy immediate threats to University ICT Services or information and communications technology security including, without limitation, suspending an Authorised User's access, confiscation of University owned electronic devices and/or disconnecting or disabling equipment with or without prior notice.

5. Consequences of Breach

5.1 Breaches of this Policy may be grounds for misconduct/serious misconduct.

5.2 Without limiting section 5.1, a breach or alleged breach of this Policy may result in a referral of the matter to the police and/or other relevant external authority.

5.3 Without limiting section 5.1, the Senior Manager, Information and Communications Technology may immediately suspend an Authorised User's account in the case of a breach or an alleged breach of this Policy.

Related Policy Instruments

Information Privacy Policy
ICT Acceptable Use Procedures
ICT Access and Account Management Procedures

Related Documents and Legislation

Singapore Statutes

The Computer Misuse and Cyber security Act (Cap 50A)
Copyright Act (Cap 63)
SPAM Control Act (Cap 311A)
Undesirable Publications Act (Cap 338)
Personal Data Protection Act 2012

Administration

Approval Details

Approval Authority:	Board of Directors
Approval Date:	02/01/2018
Version No:	V1.1
Date for Next Review:	31/12/2020

Revision History

Version	Revision Date	Description of Changes	Author
1.0	02/06/2017	Process established	Vijay Shreenivos
1.1	15/12/2017	Minor changes from American English to British English (e.g. “Authorized” to “Authorised”)	Vijay Shreenivos

Contact Person/Unit

Contact Person/Unit:	Vijay Vikram Shreenivos / Senior Manager, ICT

Keywords

Keywords:	ICT, Acceptable Usage Policy