Information Communication and Technology Acceptable Use Procedures

Intent

These Procedures have been developed to support the Information Communication Technology (ICT) Acceptable Use Policy and uphold the intent of the Policy by:

- Expressing the commitment of the University to maintaining secure, effective and reliable University ICT Services;
- Providing a clear statement of responsibilities for all users of University ICT Services, including what constitutes acceptable and unacceptable use of these services;
- Establishing clear mechanisms for rapidly responding to threats to the University ICT Services (for instance, via hacking or virus threats); and
- Providing processes to appropriately handle other security incidents, from minor breaches of Policy through to serious misconduct.

Scope

These Procedures apply to all Authorised Users of University ICT Services managed by the University or third party providers on behalf of the University, both on and off campus.

Definitions

Defined terms in the ICT Acceptable Use Policy have the same meaning in these ICT Acceptable Use Procedures.

Account means a user name or other identifier which, with or without a password, allows a user to access the University ICT Services.

Asset Owner means an individual or collective group with accountability and authority for University ICT Services.

Corrupt conduct is engaged in for the purpose of providing a benefit to the person or another person, or causing a detriment to another person. In addition, the conduct must be serious enough that, if proved, would constitute a criminal offence or a disciplinary breach providing grounds for dismissal

General Access Teaching Computer Facilities Labs (GATCF) means the computing labs and equipment provided by the University.

Inappropriate Material means content that, if accessed through University ICT Services, contravenes the Information Communication Technology Acceptable Use Policy;

ICT Bulletins means information supplied by Information and Communications Technology either by email, automatically output on a workstation or on the University websites.

Jailbreaking means the process of removing software controls on the operating systems to increase functionality or subvert security controls. Mostly commonly used when referring to Apple devices, however the concept can be applied to other makes or models.

Outside User means a person or organisation external to the University.

Private Cloud means a service operated solely for a single organisation, whether managed internally or by a third-party, and hosted either internally or externally.

Table of Contents

1. General Usage

2. Personal Computer Security

3. Software Licensing

4. Physical Security

5. General Access & Teaching Computer Facilities (GATCF)

6. Sustainability - Energy Management

7. Data Management

8. Security Management

9. System Logging and Monitoring

10. Reporting and Handling Events, Incidents or Breaches

11. Handling Breaches of ICT Acceptable Use Policy

12. Responding to Requests for Information

13. Inadvertent Unacceptable Use

Introduction

University ICT Services are the property of the University.

These procedures are designed to support the operational nature of the ICT Acceptable Use Policy by providing detailed acceptable use procedures.

Procedure

1. General Usage

1.1 Categories of Authorised Users include:

a. Any University student who has been allocated an Account or who has been authorised by a member of University academic staff to use an Account;

b. Any member of University staff who has been allocated an Account or who has been authorised to use an Account allocated to another person or to a group of people or to a section of the University. They must use University ICT Services for officially approved purposes. Limited personal use is permitted as explained in the James Cook University Code of Conduct Explanatory Statement in t;
c. Any representative of another educational institution authorised to use University ICT Services through an arrangement between the University and the other educational institution;
d. An Outside User who has been provided with an Authentication Credential; or
e. Any individual associated with an Outside User authorised to use an Account allocated to the Outside User.

1.2 Authorised Users, must:

a. Take responsibility for all activity initiated from any Account through which they have been granted access to University ICT Services;

b. Ensure that their Authentication Credential(s) are securely stored as they are responsible for all activity initiated from their Account or with their Authentication Credential(s);

c. Not allow another person to use their Account and/or Authentication Credential. Similarly, an Authorised User must not attempt to initiate or operate a computer session by using another person's Account and Authentication Credential, or by any other means. Should an Authorised User believe that the security of an Account has been compromised they must report this to the ICT Help Desk;

d. Not circumvent the University's authorised connections or subvert its security measures. This includes ‘jailbreaking’ of University owned devices;

e. Only access University ICT Services using the Accounts they have been authorised to use (kiosk services have an implicit authorisation to use);

f. Observe ICT Bulletins issued by the University; and

g. Comply with any system quotas. If an Authorised User exceeds any of their quotas, they may be personally charged for the cost of their use and/or temporarily prevented from using the affected University ICT Service.

2. Personal Computer Security

2.1 University staff and students, who use a personal computer (including smartphones) must:

a. Take responsibility for the security of personally owned computers and equipment used in conjunction with the University's ICT Services;

b. Familiarise themselves with ICT good practice guidelines (available on the Information and Communications Technology website) and take reasonable steps to ensure that personal computer(s) do not pose a threat to University ICT Services when connected to the University network. This may include:

i. Regularly scanning their device for viruses; and

ii. Maintaining up-to-date software versions; and

2.2 Protect against loss or theft of University data by:

a. Regularly backing up data;
b. Using encryption tools to protect sensitive data;
c. Logging off or locking devices when left unattended;
d. Implementing a secure access mechanism, such as a password; and
e. Avoiding leaving devices unattended in public places even if physically secured.

3. Software Licensing

The University has entered into various software licensing agreements with software vendors. Under the terms of those agreements, University staff and students may be able to install any of the products covered under the agreement onto University owned machine or personal device(s).

Refer to the Software Supplier Agreements & Offers on the University ICT Services Intranet for information on how to access software and the terms of use which must be complied with by staff and students.

4. Physical Security

4.1. Authorised or Outside Users must:

a. Take responsibility for the physical security of all University ICT Services owned or leased by their area. Where these University ICT Services are managed by Information and Communications Technology, the responsibility is shared between the Divisional Director (physical security) and Senior Manager, Information and Communications Technology (data and systems security).

4.2. Information and Communication Technology must:

a. Physically secure all University core infrastructure and GATCF Labs against theft. This can be achieved by:

i. Implementing secure cables between the device and the building; or
ii. Storing equipment in lockable rooms; or
iii. Storing equipment in lockable cabinets.

5. General Access & Teaching Computer Facilities (GATCF)

5.1. Authorised Users who use the GATCF facilities must:

a. Abide by the ICT Acceptable Use Policy, associated procedures and GATCF Conditions of Use.

6. Sustainability - Energy Management

6.1. When on a University campus, University staff and students should:

a. Save consumption of energy by powering down systems/devices when left unattended for long periods.

6.2. Information and Communication Technology must:

a. Implement power management programs to reduce the energy consumption for non-critical University ICT Services.

7. Data Management

7.1. All academic research supervisors and research Deans are responsible for ensuring that they:

a. Define research data management requirements and communicate these requirements to the relevant stakeholders; as required by the Code for the Responsible Conduct of Research.

7.2. All University staff and students must:

a. Adhere to the data management requirements as specified by their Divisions/Departments;

b. Ensure all electronically held University owned information is stored in such a way that it is backed up regularly. This can be achieved by:

i. storing data on University approved systems;

ii. storing data on a University network drive or system; or

iii. storing data on a University endorsed cloud based storage;

8. Security Management

8.1. All Asset Owners must:

a. Take responsibility for the physical security and access control of all the data stored on, transmitted through or processed by University ICT Services within their responsibility;

b. Implement suitable security controls to prevent un-authorised access or modification to data; and

c. Monitor the effectiveness of security controls to ensure their on-going effectiveness.

8.2. Information and Communications Technology must:

a. Lead and advise on good practice security management across the University. This includes providing advice and support to Asset Owners on good practice with regard to information and data security;

b. Manage common University ICT Services in such a way that the services and data are reasonably protected from:

i. Unauthorised access and unacceptable use;

ii. Common and easily exploitable vulnerabilities;

iii. Wilful, malicious damage or any activity undertaken to intentionally bypass security controls on University ICT Services; and

iv. Virus infection and malicious software;

c. Take reasonable steps to ensure that data on University ICT Services is:

i. Accurate and complete;

ii. Available to be accessed by Authorised Users, and only those users, when required; and

iii. Recovered in an agreed timeframe in the event of serious systems failure or disaster;

d. Ensure required University owned or leased computers, desktops or laptops are configured to have a password enabled screensaver that activates within a period of no greater than 30 minutes of inactivity;

e. Promote a positive and safe computing environment for all Authorised Users;

f. Implement appropriate quotas on the use of University ICT Services (this may include print, file storage, email and internet usage) in order to ensure the ongoing integrity and availability of University ICT Services;

g. Ensure sensitive information is disposed of in a manner that renders any information illegible and irretrievable at the time of disposal by:

i. Physically destroying the media;

ii. Bulk wiping (degaussing); or

iii. Implementing an industry approved 3-times secure wipe of the media; and

h. Carry out security reviews of University ICT services to verify the on-going effectiveness of controls. This should include access reviews of administrative accounts.

9. System Logging and Monitoring

9.1. Information and Communications Technology will:

a. Implement appropriate logging of use of University ICT Services and routinely monitor to assist in the detection of breaches of these Procedures and the ICT Acceptable Use Policy.

b. Monitor the use of University ICT Services and investigate potential breaches of University Policy, or State Law.

10. Reporting and Handling Events, Incidents or Breaches

10.1. All Authorised Users must:

a. Report any actual or suspected security weakness, breach or threat involving University ICT Services to the ICT Help Desk or the Senior Manager, Information and Communications Technology as soon as possible;

b. Respond to potential incidents or events, including un-authorised system usage, as directed by an Information and Communications Technology staff member; and

c. Report lost, stolen or damaged University owned computers or other equipment to the ICT Help Desk and Singapore Police Force for the First information report.

10.2. Information and Communications Technology must:

a. Respond to potential incidents, events, breaches or requests for information (as per Section 12). Responses may include, but are not limited to:

i. Modifying University ICT Services;
ii. Taking reasonable steps to protect University ICT Services from un-authorised or unacceptable use. This may include suspending Accounts, confiscating University owned electronic devices and/or disconnecting or disabling relevant services or other equipment, with or without prior notice;
iii. Handle alleged breaches in accordance with Clause 11; or
iv. The retrieval or examination of documents or messages for purposes such as finding lost files or messages, complying with legal requests, or recovering from system failure.

11. Handling Breaches of ICT Acceptable Use Policy

If an alleged breach of the ICT Acceptable Use Policy is reported to the ICT Help Desk or the Senior Manager, Information and Communications Technology will conduct a preliminary evaluation of the allegation. Any alleged breach that may also constitute Corrupt Conduct will be referred, in the first instance, to the Director, Operations. Similarly, any disclosure by a person of an alleged breach that may constitute a Public Interest Disclosure must also first be referred to the Director, Operations.

Following the preliminary evaluation, the Senior Manager, Information and Communications Technology may:

a. Dismiss the matter if the allegation is deemed to be unfounded or trivial, and send written advice of the dismissal and reasons for the dismissal to the complainant or appropriate officer;

b. In the case of an alleged breach by a University student refer the matter to the Director, Operations to be dealt with under the Student Code of Conduct or other appropriate University policies;

c. In the case of an alleged breach by a University staff member or adjunct refer the matter to the Director, Human Resources (or Deputy Vice Chancellor if Director, Human Resources is alleged to have committed the breach) to be dealt with in accordance with the terms of the applicable Enterprise Agreement and/or appointment document;

d. In the case of an alleged breach by an Executive Management Group member, the issue will be dealt with in accordance with the James Cook University Code of Conduct;

e. In the case of an alleged breach by an Outside User, refer the matter to the University Authorised User who is responsible for the Outside User to be dealt with by that University Authorised User; and/or

f. In the case of an alleged breach by a student or staff of another educational institution authorised to use University ICT Services through an arrangement between the University and the other educational institution, refer the matter to the relevant educational institution to be dealt with by that institution.

12. Responding to Requests for Information

12.1. Information and Communications Technology must respond to all requests to access records relating to ICT Services received from the Executive Management Group.

12.2. Subject to paragraph 1 above, Information and Communication Technology may only respond to requests to access records relating to ICT Services, as follows:

a. In so far as the request relates to staff or students, from the Deputy Vice Chancellor and Head of the Singapore Campus; Director of Compliance (Director Internal Audit and Standards) or Director of Human Resources;

b. In so far as the request relates to student records, from the Director, Operations;

c. In so far as the request relates to staff or adjunct records, from the Director, Human Resources;

d. In so far as the request relates to University Council to the Board, from the Director Operations.

13. Inadvertent Unacceptable Use

Authorised Users, who inadvertently receive, transmit or access material (for example, via email or the Internet) that may be considered Inappropriate Material and is not related to their work duties, must take immediate action to either delete such material or cease such access.

Advice must be sought from the Authorised User's supervisor or the ICT Help Desk if Inappropriate Material continues to be received.

Related Policy Instruments

Code of Conduct
ICT Acceptable Use Policy
ICT Access and Account Management Procedures
ICT Asset Management Policy
Information Privacy Policy

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:	Deputy Vice Chancellor
Approval Date:	01/04/2017
Version No:	V1.0
Date for Next Review:	31/12/2017

Revision History

Version	Revision Date	Description of Changes	Author
1.0	01/04/2017	Process established	Vijay Shreenivos

Contact Person/Unit

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

Keywords

Keywords:	ICT, Acceptable Use Procedures