Acceptable Use of Information and Communications Technology (ICT) Resources (2019)

Purpose: The University of Seychelles (hereafter, UniSey) seeks to provide its information and communications technology (ICT) users with secure and timely access to ICT equipment and the online services and resources necessary for undertaking their work and study. This policy sets out the rules applicable to the use of University ICT and expresses the commitment of the University to providing and maintaining a secure, effective and reliable ICT infrastructure and services to support the University's operations.

Definitions:

1. User/s include:

- Students
- Staff, whether full-time, part-time, ongoing, fixed-term, casual or sessional.
- Visiting and adjunct academics, or other academic or research collaborators.
- Individuals who have been granted access to UniSey facilities (e.g. Conference attendees at UniSey venues).
- Committee members or volunteers who contribute to or act on behalf of the University.

2. UniSey ICT Resources: All of the University's Information and Communication Technology Resources and facilities including, but not limited to: mail, telephones, mobile phones, voice mail, SMS, email, student database, the intranet, computers, printers, scanners, access labs or other facilities that the University owns, leases or uses under Licence or by agreement; any off campus computers and associated peripherals and equipment provided for the purpose of University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks.

SCOPE AND APPLICATION This policy applies to all users of University ICT Resources. All users of the University's ICT resources have a responsibility to only use those resources in accordance with the requirements of this policy. This policy also applies to users connecting personally owned devices such as laptop computers, smartphones and tablets to the University network, and/or storing any University data on such devices.

POLICY PRINCIPLES:

3.1 Principles

(1) The University’s ICT Resources exist and are maintained to support the work of the institution. UniSey recognises that ICT resources may be used for incidental personal use. The University reserves the right to monitor the use of its ICT Resources and to deal appropriately with Users who use its ICT Resources in ways contrary to the conditions of use set out in this policy.

(2) Materials produced using the University’s ICT Resources are to be generated subject to the relevant University recordkeeping policies.

(3) The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources. It is recommended that users regularly back up their data especially when handing over their computer for maintenance.

(4) This policy sets out the University's behavioural expectations for the use of its ICT resources. The use of all ICT resources is monitored and any unacceptable use will be investigated.

3.2 Acceptable use of information technology resources

Acceptable use of the University's ICT resources will:

1. be consistent with national laws[1]
2. be consistent with the University's behavioural expectations as defined in the Human Resources Manual and the Student Policy.
3. be within any quota or cost limit imposed by the University.
4. maintain the security of the University's ICT resources and facilities.
5. ensure that users adhere to the terms and conditions of all license agreements relating to any software installed on or accessed by, University computers including restrictions for commercial use.

3.3 Unacceptable Use of ICT Resources.

Users must not use University ICT as follows:

1. to engage in harassing, cyberstalking or other anti-social behaviours on-line; to transmit material that is threatening, violent, abusive, hateful, discriminatory, defamatory and invasive of another’s privacy.
2. to create, download, upload, store or transmit any pornographic/ obscene/ offensive material in any form.
3. to attack or gain unauthorised access to other network, computer systems of data;
4. to transmit unsolicited bulk email (spam).
5. for excessive personal use; transmitting graphic-rich (e.g., gaming), music and video files or software for personal use, is not authorised.

6. to save personal software or graphic-rich music and video files to any network drive.
7. to infringe the copyright of another person or organisation.
8. to purposely install malicious software such as viruses, worms or address-harvesting software and to click open unknown links and attachments.
9. to connect laptops to the UniSey network, which do not have adequate protection against virus or malware.
10. to gain any inappropriate personal, academic or other advantage;
11. to maintain or support a personal private business;
12. Users must not remove ICT equipment from the University. Users disconnecting a network cable from a University computer to plug into a device must reconnect the cable.

3.4 Inadvertent unacceptable use

Users who inadvertently receive or access unacceptable material must take immediate action to either delete such material or cease such access. Advice should be sought from IT Services if unacceptable material continues to be received.

3.5 UniSey access account

A user is responsible for any activity, transaction or publication of information which originates from their UniSey access account. A user must not undertake any act which prejudices the security of their UniSey access account including disclosing their password to any other person or allowing any other person to use their account. Passwords must be selected using good security practices, highlighted in the UniSey Password Security Guidelines, annexed herewith (Annex 1). University email accounts are not for personal use (i.e., signing up to websites and effecting communications on a private basis).

UniSey communicates with staff and students via their University email accounts. Users are expected to access these on a regular basis and manage their accounts appropriately.

3.6 Incidental personal use

UniSey recognises that ICT resources may be used for incidental personal use (outside of work or approved study purposes). Incidental personal use must be infrequent and minor, and must not breach this policy or interfere with University business operations or the performance of a staff member's duties. Incidental personal use of the University's ICT resources does not include any of the following:

1. maintaining a private business
2. recruitment of members to, or soliciting donations for political parties
3. the transmission, viewing or publication of unacceptable material
4. publication of internet sites or pages unrelated to University activities
5. personal comments using offensive language
6. a malicious or unlawful purpose.

4. Monitoring and detection

The University reserves the right to audit regularly and monitor the use of its ICT Resources to ensure compliance with this policy. The University also reserves the right to inspect any information, data or files (including non-University material) created, sent or received by users using, or while connected to, the University's ICT Resources in the event of a suspected breach of this or other policies. While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the privacy or security of any information. Where the alleged breach presents a risk to the University, IT Services may implement immediate technological measures to mitigate the risks.

4.1 Procedure for handling breaches

a) If an alleged breach of the Acceptable Use of ICT (Section 3.3) is detected by or reported to Information Technology Services (ITS), Information Technology Services Director will refer the alleged breach to the University Registrar for a decision on what further action should be taken in respect of the User.

(b) The University reserves the right to withdraw, restrict or limit any User's access to its ICT Resources if a breach is suspected. Any such suspected breach may also be investigated under other University processes, and may result in disciplinary action being taken against the offender in accordance with those processes. This may include a request to reimburse costs (e.g., for unreasonable personal use), disciplinary action (including termination of employment/suspension of candidature) and /or criminal prosecution.

(c) UniSey reserves the right to remove or restrict access to any material within the University domain. Such decisions will be communicated to the appropriate supervisor and account holder.

(d) The University has a statutory duty to co-operate with the Police in the course of an investigation, allowing access to a user's email, file spaces and any logged information, where a warrant is properly executed in relation to an investigation.

[1] Computer Misuse Act,1998

Electronic Transactions Act, 2001

Digital Signature Regulations, 2018

Seychelles National ICT Policy http://www.ict.gov.sc/resources/policy.pdf

Annex 1

UniSey Password Security guidelines for staff and students

These guidelines must be read in conjunction with the University of Seychelles Information Technology Policy (2019), particularly article 3.5 (UniSey access account), which states:

A user is responsible for any activity, transaction or publication of information which originates from their UniSey access account. A user must not do any act which prejudices the security of their UniSey access account including disclosing their password to any other person or allowing any other person to use their account. Passwords must be selected using good security practices, highlighted in the UniSey Password Security Guidelines.

Note to staff and students

- When your account as staff or student is first set up, you will be assigned with a generic password, which you will have to change immediately.
- To change your account password, press Alt/ Control/ Delete keys to get to the Microsoft Control screen. Select ‘change a password’ option.

UniSey password requirements – all UniSey passwords must contain:

- at least eight (8) characters.
- a combination of at least 3 of the following:
  - lowercase letter
  - uppercase letter
  - number
  - a special character such as !@#$%^&*()[]\;',./{}|:"<>?

Creating a Strong Password

- Stay away from the obvious. Never use sequential numbers or letters, and do not use the word *password*. Come up with unique passwords that do not include any personal information such as your name or date of birth.
- The longer the better.
- Use a mix of characters — The more you mix up letters (upper-case and lower-case), numbers, and symbols, the stronger your password is, and the harder it is for a hacker to crack it.
- Avoid common substitutions: Whether you use DOORBELL or D00R8377, a hacker can crack it with ease.

Resetting Your Password

- Passwords expire after 90 days and need changing. You will be prompted when you log into UniSey domain account.

- You can change your password more frequently for peace of mind.
- Use a strong password that meets the above policy requirements.
- Each time you change your password, verify that you can access all of your systems and services.