COVENANT UNIVERSITY POLICY ON ICT FOR FACULTY/STAFF AND STUDENTS

2016 – 2019

119th Senate (S.119/1556) – Thursday, February 18, 2016

PREAMBLE

In accordance with the National Universities Commission's guidelines, Covenant University's (CU) Senate has set out these ICT minimum guidelines for proper, efficient and effective use of ICT in achieving its mission and objectives. To this end, these minimum guidelines would articulate the framework, and the course of action that guides acceptable use of ICT facilities and resources by all members of the University community. This policy applies to all equipment owned or leased by Covenant University, and to all equipment connected to the Covenant University network.

1. PURPOSE

The main purpose of the ICT Policy is to harness the potential of ICT as a catalyst for effective learning, teaching, research and innovation in Covenant University for national transformation, global competitiveness and raising new generation of leaders. It outlines the **acceptable** and **unacceptable** use of computer equipment or "online services" owned by Covenant University. The objectives of the ICT policy are specifically to:

1.1. Provide guidance in developing a broad based, reliable and secure communications infrastructure, which shall conform to recognised international standards and support all services in the University.

1.2. Provide a framework for development and management of ICT network services that shall ensure the availability, enhanced performance, security, and ensure the reduction of the cost of running ICT infrastructure.

1.3. Provide a framework, including guidelines, principles and procedures for the development and implementation of ICT projects in Covenant University.

The provisions of this ICT Policy, which are outlined in sequel sections, cover the following areas:

a. Applications of ICT to Education Delivery at Covenant University

b. Applications of ICT to Administration in Covenant University
c. Infrastructure
d. Network Development and Management
e. Access Management and Control
f. Capacity Building
g. ISO Information Security Management Systems
h. Equal Opportunities
i. Maintenance of ICT Facilities
j. Collaborative Services and Resource
k. World Web Universities Ranking

2. DEFINITION OF TERMS

2.1. **Computing services** refer to any IT resource made available to an individual, any of the network borne services, applications or software products that an individual is provided access to and the network/data transport infrastructure that an individual uses to access any of the services (including wired and wireless access to the Internet).

2.2. **Online services** include services provided and accessible (both wired and wireless) through individual accounts and passwords. Such services include access to internet/intranet related systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, internet browsing, and FTP and are the property of Covenant University.

2.3. **Devices** include but are not restricted to computer desktop, laptops, mobile tablets and smart phones.

3. UNACCEPTABLE USAGE: This may be summarised as, but not restricted to:

3.1. Actions, which cause physical damage to any ICT hardware and software, including peripherals (e.g. mouse, cables, wiring, printers, etc.).

3.2. Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, inappropriate or likely to cause offence.

3.3. Threatening, bullying, intimidating or harassing staff, students or others.

3.4. Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.

3.5. Defamation
3.6. Unsolicited advertising often referred to as "spamming".

4. ICT ELECTRONIC MESSAGING

4.1. The Covenant University electronic messaging services shall be used in an appropriate and responsible manner.
4.2. Covenant University shall permit users to use electronic messaging services in an appropriate and responsible manner.
4.3. A user's access to electronic messaging service shall be withdrawn the moment his/her affiliation with the University as a staff, student or associate ceases.
4.4. All records created by university staff during the course of university business shall be owned by Covenant University as corporate assets.
4.5. All users of electronic messaging services shall be aware of their responsibilities with regard to the creation, capture, retention and disposal of university records.
4.6. An electronic messaging user shall act in a *professional and ethical manner*.
4.7. A user shall maintain professional courtesies and considerations in all electronics communication.
4.8. A user shall not transmit abusive or defamatory messages.
4.9. A user shall not transmit an electronic message that breaches legislation (such as the spam Act 2003) or contravenes Covenant University policy.
4.10. A user shall not cause interference to other users of electronic messaging services. Examples of interference include transmission of email, chain/bulk letters, wide spread distribution of unsolicited email, junk mail, pyramid mail and the repeated sending of the same message.
4.11. A user shall not give the impression that he/she is representing, giving opinion or making statements on behalf of Covenant University, unless authorised to do so.
4.12. Users who contravene these guidelines shall be subject to the provisions of the Covenant University ICT breach management (see Section B).

5. ICT BREACH MANAGEMENT

5.1. Any noticeable or reported breach shall be investigated to determine whether it was accidental or deliberate in order to determine the most appropriate action to be taken.
5.2. Users who are found to have breached Covenant University ICT policy shall face disciplinary measures.
5.3. Management of a breach of policy shall be determined by the facts of matter.

5.4. Penalties shall be applied in line with university misconduct processes set out in the applicable employment instrument, contract of employment or university status and may include:

5.4.1 suspending the user's university access to ICT facilities

5.4.2 withdrawal of benefit

5.4.3 dismissal

6. COVENANT UNIVERSITY PRINTING

In order to promote the responsible and ethical use of printers, printing software, or printing supplies by faculty, staff, students and other authorised users, the following guidelines shall subsist regarding printing in the Laboratories, Classrooms, Library, or at Public Sites in Covenant University:

6.1. The Centre for Systems and Information Services (CSIS) shall make purchases on printing through the Purchasing Committee with tender; installs and supports computer systems and peripherals, public site printers and printing softwares.

6.2. The University Centralised sites and Enterprise printers, Laboratories and offices shall provide papers and toners.

6.3. The public site and classroom printers shall be primarily for students, Faculty/Staff use.

6.4. Departments, Directorates and Units shall be provided with printers for security reasons.

(A) Responsibilities of CSIS on Printing with University's Equipment

The CSIS shall:

i. act as a responsible steward of University resources as it relates to printers, printing software, and printing supplies;

ii. lead, or take part in initiatives that promote sustainable practices such as decreasing printing or reducing waste;

iii. set printing standards, limits, allowances, or pricing;

iv. evaluate, select, install, monitor, maintain, and replace on a reasonable refresh cycle, any printer, printing software, or printing supplies;

v. maintain user accountability requirements, including user identification and authentication, account administration, and password integrity;

vi. develop and implement security policies and standards;

vii. ensure that printing supplies are replenished; and

viii. properly destroy or shred any unclaimed printouts or papers in its domain.

(B) Responsibilities of the Members of the University community

All members of the Covenant University community shall:

i. act in a responsible, ethical, and legal manner in the use of printers, printing software, or printing supplies (including copyright law). This use implies consent with any and all applicable university policies and regulations;
ii. refrain from using printers, printing software, or printing supplies for personal, unauthorised uses, or any other use that does not conform to Covenant University's mission;
iii. avoid any unauthorised usage of printers, printing software, or printing supplies. These include, but are not limited to, the transmission of abusive or threatening material or using printers, printing software, or printing supplies in violation of applicable license agreements;
iv. refrain from damaging or stealing printers, printing software, printing supplies, or any related technology;
v. not perform any acts, which are wasteful or monopolise printing resources, including printing unnecessary output or printing multiple copies of documents such as resumes, theses, or dissertations; and
vi. use only CSIS-approved printing resources and avoid printing on transparencies, labels, or special papers (large format, irregular thickness, etc.) that may inadvertently damage the printers.

7. DATA PROTECTION

The University's position on disclosure of information/ information in transit is as follows:

7.1. All Faculty/Staff and students of the University shall be notified of the reasons why their information will be held in the University's database, how it will be used and the institutions or establishments that the University might share such information with.
7.2. The personal data obtained from Faculty/Staff and students shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are being requested.
7.3. The Faculty/Staff and students of the institution shall have the right to access data or information held concerning them, subject to approval from the University Management.

7.4. Access to an individual's personal information shall not be given to persons other than the individual concerned or other authorised personnel except where there is a statutory requirement to do so.

(A) Data and Information Accuracy, Retention and Security

i. The accuracy and correctness of Data and Information on Faculty/Staff and students shall be ensured at all times by carrying out periodic updates of staff and students information.
ii. Records of Faculty/Staff and students shall be properly maintained and protected.
iii. Measures shall be taken to ensure that all information and software are removed from redundant hardware before it is retired or decommissioned.
iv. Expired confidential information stored on paper shall be *shredded* or *held in a secure area* in preparation for incineration.

(B) Backup and Disaster Recovery Plan

i. The Director of CSIS shall put in place a viable backup policy.
ii. The backup arrangement shall contain the following*: Disaster recovery plan; Downtime classification and Recovery schedule*.

8. PHYSICAL ACCESS CONTROL AND SURVEILLANCE

8.1. The Director of CSIS shall ensure that only authorised staff or personnel are granted access to server rooms, computer labs and other major ICT facilities of the university.
8.2. The rooms or spaces housing equipment shall be adequately secured as the doors, windows and the keys or access codes to these rooms shall reside only with the Director of CSIS or appointed representative.
8.3. Assets Register shall be maintained by all Units in CSIS to keep track and take inventory of all hardware and software in the Department.
8.4. A central register shall also be maintained by the CSIS to keep inventory of the computer equipment in the University.
8.5. All ICT equipment shall be labelled and/or engraved appropriately for identification.
8.6. All entrances to secured areas shall be appropriately labelled "*Only Authorised Persons are allowed*".

8.7. Access controls and security surveillance equipment like CCTV cameras shall be installed and monitored in secure areas to prevent unauthorised access, theft and tampering with computing facilities during and after working hours.

9. INTERNET USAGE

Access to the University's network facilities (wireless and wired) shall be controlled through the following measures:

9.1. All Faculty/Staff and students shall be provided with a username and password etc, to be able to access the computer systems and the internet. The naming convention shall be adhered to.

9.2. All students shall be allowed access to the Internet network facilities from *4 a.m. to 12 midnight daily*.

9.3. All traffic passing through the firewall shall be screened and audited.

9.4. CSIS shall maintain control over data packets and connection requests by means of a centralised firewall that will adequately filter data traffic.

9.5. In line with the Covenant University Core Values, all authorised users shall not be allowed to view or visit sites with offensive and inappropriate materials (e.g. *pornographic sites, sites used to spread hate and racial or religious intolerance, etc.*).

9.6. Defaulting users shall have their user names and passwords disabled and penalised appropriately.

9.7. All users shall not download or upload offensive materials on the University's network.

9.8. To optimise students' level of academic productivity, the University reserves the right to restrict their access to certain/specific websites for a certain period of time as may be conserved necessary.

10. ANTI-VIRUS

The University shall activate and use encryption services with anti-virus protection in all cases where a device requires such services.

11. ANTI-PIRACY

The University shall not tolerate unlicensed or pirated software on her network in order to respect ownership of Intellectual Property rights and avoid litigation.

12. HARDWARE MAINTENANCE AND MANAGEMENT

12.1. The University shall make provision for adequate resources to ensure regular maintenance of ICT equipment (computers, servers, etc.).

12.2. The University shall also refurbish or replace obsolete and outdated computer laboratory equipment as early as possible to minimise maintenance cost and incompatibilities.

12.3. The University shall systematically modernise her stock of computers to meet the demands of latest software, web access and other tasks of computation and communication.

12.4. A maintenance programme shall be put in place to ensure that the hardware devices are serviced and replaced from time to time.

12.5. CSIS shall maintain and support all hardware devices/peripherals (which may include desktop computers, laptop computers, printers, scanners, digital cameras, projectors, power backup systems and network equipment) in the University.

12.6. Users of the hardware shall strictly adhere to the guidelines on ICT usage of the hardware in order to guarantee support by CSIS.

13. INFORMATION SYSTEMS SECURITY

In order to ensure information system security, a user shall be responsible for the following:

13.1. Become familiar with the device that is sufficient to keep data secure.

13.2. Prevent theft and loss of data (using PIN/Password/Passphrase lock).

13.3. Keep information confidential, where appropriate.

13.4. Maintain the integrity of data and information.

13.5. Never retain personal data on University's systems.

13.6. When in doubt as to whether particular data can be stored on the device, ask/consult with the Director of CSIS or seek advice from the appropriate authority.

13.7. Staff shall not be encouraged to keep University data in their personal systems/devices.

13.8. All official communication shall be routed through the University e-mail.

13.9. No one shall delete official documents from the University's systems in their care, negligently or deliberately.

14. E-LEARNING

14.1. The University shall adopt and enforce the e-learning method for education delivery through the creation of an e-Learning Working Committee.

14.2. The primary duties of the e-Learning Working Committee shall be to make recommendations on online teaching and learning.

14.3. Other duties of the e-Learning Working Committee shall be to:

14.3.1. Conduct periodic review of development of e-learning in the University;

14.3.2. Create guiding principles for e-learning;

14.3.3. Review the key collaborations /partnership with other institutions;

14.3.4. Create a roadmap for Covenant University Massive Open Online Courses/Courseware (MOOC); and

14.3.5. Conduct periodic quality assurance and evaluation of sharing in Covenant University.

14.4. To support student's e-learning method, the University shall:

14.4.1. ensure that lecture notes and pre-recorded lecture videos are available online for students engaged in e-learning activities;

14.4.2. provide facilities for students to submit their coursework and assignments electronically;

14.4.3. provide for the students to have unfettered correspondence with their Lecturers via emails, school intranet or Departmental Portals. This correspondence shall include ability to apply for test rescheduling, extenuating circumstances, review and questions on projects and coursework;

14.4.4. ensure students have access to Library resources and e-Journals without having to be physically present on the campus;

14.4.5. ensure students are able to access test scores, grades, financial status and lecturer's comments on the University's Portal;

14.4.6. ensure that every lecturer and teaching staff has access to a computer and internet services;

14.4.7. have a well-stocked computer laboratory accessible to all registered students, Faculty and staff;

14.4.8. ensure that every incoming undergraduate into the University has a laptop and or a mobile device; and

14.4.9. provide platform for Covenant University Lecturers to implement MOOC on e-learning.

15. SYSTEM AUDIT AND INVESTIGATION

15.1. If any computer system or facility is threatened, it shall be monitored and user files shall be examined under the directive of the Vice-Chancellor.

15.2. The University shall comply with all governmental and law enforcement orders requiring the examination of user files. This may occur if:

15.2.1. there is reasonable cause that a user has violated this policy;

15.2.2. a user or an account appears to be engaged in unusual activity;

15.2.3. it is necessary to protect the integrity, security, or functionality of Covenant University's technology resources;

15.2.4. it is necessary to protect Covenant University from liability; or

15.2.5. it is required by law.

16. ENFORCEMENT AND DISCIPLINARY PROCEDURES

Any user who violates any part of this policy shall be subjected to the following:

16.1. Suspension or revocation of the user's computer account and/or suspension or revocation of access to the University's printing resources.

16.2. Disciplinary action as described in Covenant University's Student Handbook.

16.3. Disciplinary procedures outlined in Covenant University's Staff Handbook or any other documents outlining conduct for Faculty, Staff and students.

16.4. Civil or criminal prosecution under federal and/or state law.

17. PROCEDURE TO UPDATE THE POLICY

17.1. Covenant University reserves the right to update and/or amend this document to reflect University policy changes and/or state or federal law.

17.2. Ignorance of this policy (or those that it directs individual to), and the responsibilities it places on individual, shall not be an excuse in a situation where it is assessed that an individual has breached the policy and its requirements.

17.3. Students, Faculty/Staff who connect their own devices to the University network and the services available shall be reminded that such use requires compliance to this policy.

17.4. Students shall be informed of this policy during their induction each year and shall acknowledge their readiness to adhere and comply with the policy each time they log on to the University network.

17.5. Staff members shall be informed of this policy during their induction and the need to adhere to the conditions therein.

18. VENDORS PROCUREMENT REPOSITION

The expected detailed plan to be submitted by Vendors shall include the following:

- 18.1. Table of Content
  - 18.1.1. Document Information
  - 18.1.2. Authors
  - 18.1.3. Contributors
  - 18.1.4. Scope of Work
  - 18.1.5. Project deliverable
  - 18.1.6. Defined method of approach
- 18.2. Equipment for supply
- 18.3. Exclusion
- 18.4. Interfaces
- 18.5. Service Level Agreement
- 18.6. Trade Off arrangement
- 18.7. Form of Indemnity
- 18.8. Equipment certification (OEM)
- 18.9. Maintenance and Implementation Process