

***UNIVERSITY OF SIERRA LEONE  
INFORMATION AND COMMUNICATION POLICY  
OCTOBER 2018***

# University of Sierra Leone ICT Policy - 2018

---

## Table of Contents

1.0 Policy Statement.....	4
1.1 General Scope .....	4
1.2 ICT Governance .....	5
1.2.1 The Directorate .....	5
1.3 ICT Resources .....	6
2.0 Acceptable Use.....	6
2.1 Unacceptable Use .....	7
3.0 Electronic Mail & Messaging Services.....	7
3.1 Ownership and Responsibilities .....	7
4.0 Copyright Laws and License Agreements.....	7
5.0 Authorized Users .....	8
6.0 Use of Email Accounts .....	8
6.1 Email Content.....	8
6.2 Creation of Messages .....	8
6.3 University Records .....	8
6.4 Offensive Electronic Content .....	9
7.0 Responsible use of ICT Resources .....	9
7.1 Restrictions.....	9
7.2 Misrepresentation .....	10
7.3 Personal Use.....	10
8.0 Security and Confidentiality.....	10
8.1 Privacy .....	10
8.2 Security and Protection .....	11
8.2.1 Declaration .....	11
9.0 ICT Security.....	11
10.2 Roles of Campus ICT Services Unit .....	12
12.0 Physical Security & Integrity of Systems .....	12
13.1 Software and Firmware upgrades .....	13
13.2 Malware control.....	13
13.3 Network Interconnections .....	13
14.0 Privacy and Confidentiality.....	13
14.1 Right to Monitor ICT Systems .....	14
15.0 Localized Policies .....	14

# University of Sierra Leone ICT Policy - 2018

---

16.0 Social Media.....	14
16.1 Definition of Concepts .....	15
17.0 General Liability.....	16
18.0 Use of USL Marks .....	16
18.1 Compliance with other USL policies .....	17
18.2 Penalties for Misuse.....	17
Annexes .....	18
Bibliography .....	20

# University of Sierra Leone ICT Policy - 2018

---

## 1.0 Policy Statement

This Policy outlines the guidelines on Information and Communication Technology (ICT) management in the University of Sierra Leone (USL).

## 1.1 General Scope

This policy covers all aspects of the ICT resources wherever located. The policy is binding on all users of ICT resources of the USL. Users of the University's ICT resources have access to sensitive data and external networks. Consequently, it is important that they use these resources in a responsible, ethical and legal manner.

The Information and Communication Technology (ICT) policy applies to all University of Sierra Leone constituent Colleges, Departments, and Units and covers but not limited to following areas:

- I. University of Sierra Leone ICT Governance
- II. University of Sierra Leone ICT Resources
- III. Acceptable use of ICT Resources
- IV. Unacceptable use of ICT Resources
- V. User Acceptance
- VI. Electronic Mail & Messaging Services
- VII. Ownership and Responsibility
- VIII. Authorized Users
- IX. Use of E-mail Contents
- X. Responsible use of ICT Resources
- XI. Security and Confidentiality
- XII. ICT Security
- XIII. Qualifying Users
- XIV. Physical Security and Integrity of Systems
- XV. Logical Security and Integrity of Systems
- XVI. Privacy and Confidentiality
- XVII. Localized Policies
- XVIII. Social Media
- XIX. Definition of Concepts

# University of Sierra Leone ICT Policy - 2018

---

XX. Statement of Liability

XXI. Penalties for Misuse

## 1.2 ICT Governance

ICT governance is an active and ongoing function that requires adequate and sustained funding.

USL shall ensure the provision of resources within the University Budgeting process for the provision and maintenance of University wide ICT infrastructure and services.

Ring fence proceeds from the sale of electronic ID cards for the sustenance of services provided by University portal

Allocate one percent (1%) of all University Grants to ICT support.

### 1.2.1 The Directorate

The Directorate shall constitute a minimum of a Director, Deputy Director and a manager each for the campuses. Each campus manager shall be supported by minimum of four relevant technical staff

The Directorate for ICT Support shall:

- a) Provide effective ICT support to the academic, research and administrative functions of the University
- b) Promote effective and appropriate utilization of ICT resources
- c) Promote an environmentally friendly approach to the acquisition, use and disposal of ICT resources
- e) Coordinate and undertake resource mobilization for counterpart funding for the implementation of the ICT Strategy.
- f) Specify, verify and vet ICT standards, procedures and best practices for all University ICT deployments and operations.
- g) Have the overall ownership of the professional and technical mandate of all ICT design and developments, management and maintenance.
- h) Operationalize and guide the ICT policy implementation.
- i) Advise the University administration on ICT policy review
- j) Ensure quality assurance compliance
- k) Establish and manage user forums for end users
- l) Integrate ICT into the operations of USL at all levels
- m) Ensure that the USL ICT policy conforms with national and international ICT polices and standards

# University of Sierra Leone ICT Policy - 2018

---

## 1.3 ICT Resources

The ICT resources of the USL include but not limited to the following:

- i. Hardware
- ii. Software
- iii. Networking equipment, services and facilities
- iv. Communication equipment, services and facilities
- v. Data and information
- vi. Relevant Cloud-based resources and services

This policy applies to all ICT resources owned, leased or loaned by USL or its agent irrespective of where they may be located. Access to USL ICT resources is conditional on the observance of this policy.

Examples of these ICT resources include, but are not limited to:

- i. Central computing facilities.
- ii. Enterprise software applications
- iii. The Campus Area Network (CAN)
- iv. The University WAN(Wide Area Network
- v. Local Area Network(LAN)
- vi. Electronic mail
- vii. Internet access
- viii. Internet and Intranet Web servers
- ix. Web pages
- x. Public computing facilities
- xi. Voice telephony systems
- xii. Wireless network systems
- xiii. Human resource data
- xiv. Student data
- xv. Learning and teaching platforms and systems

## 2.0 Acceptable Use

The University recognizes the following as acceptable use:

# University of Sierra Leone ICT Policy - 2018

---

- University information systems are to be used solely for University-related business, inclusive of teaching and learning processes.
- Personal use of ICT facility should be authorized by the University through the Directorate

## **2.1 Unacceptable Use**

The University recognizes the following as unacceptable use:

- ICT use must not conflict with the aims and objectives of the University of Sierra Leone
- Unauthorized use of ICT resources including politically sensitive statements, propagation of hate speech, indecent and unethical exposure etc.
- Violation of national laws

## **3.0 Electronic Mail & Messaging Services**

- Promote the use of electronic mail services to share information, improve communication, and to exchange ideas.
- The USL electronic mail, messaging services and collaborative platforms shall be the official means of electronic communication

## **3.1 Ownership and Responsibilities**

- All data generated through the use of USL electronic facility shall be the property of the University unless otherwise specified
- Electronic messaging services are provided by the USL to support the operational and administrative functions of the USL - teaching, learning, research, and the management of the USL's business. It is intended to be used primarily as a business tool.

## **4.0 Copyright Laws and License Agreements**

- USL shall respect the provisions of its Policy on Intellectual Property and the users of the system shall observe this Policy and all applicable copyright laws and license agreements.

# University of Sierra Leone ICT Policy - 2018

---

## 5.0 Authorized Users

- Users of University Electronic Messaging Services are to be limited to USL students, faculty, staff and other approved persons, for purposes that advance the objectives of teaching, learning, research, outreach and administration.

## 6.0 Use of Email Accounts

- All email accounts shall conform to the information security procedures defined and implemented from time to time and managed by campus ICT Directorate.
- Passwords should not be given to unauthorized persons.
- Access to university electronic mail services, when provided, is a privilege that may be wholly or partially restricted by order of the Competent University Authority without prior notice and without the consent of the e-mail user when there is substantiated reason to believe that violations of policy or law have taken place. Such restriction as applied is subject to review by the appropriate superior university authority.

## 6.1 Email Content

- The content of electronic messages qualifies as recorded material and is subject to the same rules and regulations as any other type of record created, used, or received and retained by the University throughout the course of business.

## 6.2 Creation of Messages

- The same rules governing good sociable behavior applying to face-to-face communication or to traditional written communication, apply also to electronic communication. Messages should reflect careful, professional and courteous drafting, particularly since they are easily forwarded to others. It is advised that every user of university email systems assume that others apart from the addressee[s] may read a message.

## 6.3 University Records

- Messages sent or received on behalf of the University and which provide evidence of an activity, transaction or event must be regarded as official University records. Such records must be retained in an official repository. Their disposal must be in

# University of Sierra Leone ICT Policy - 2018

---

accordance with approved retention and disposition schedules. Records relative to matters subject to on-going or threatened legal action or any investigation must be retained and should not be disposed of, even if the retention period has been met on the records retention schedule, except as advised by the University Legal Counsel.

## 6.4 Offensive Electronic Content

- It is strictly prohibited to send harassing, abusive, intimidating, discriminatory or other offensive electronic messages including vulgar and pornographic content.
- It is a misuse of the facilities, and may in certain cases, be illegal for a user to receive, transmit, display or store such offensive material using University equipment. Such misuse may result in disciplinary or legal action being taken against those responsible.

## 7.0 Responsible use of ICT Resources

- Users of university electronic messaging systems are expected to exercise sound judgment and caution when distributing e-mail messages.
- All users are advised to follow the guidelines accompanying these policies and use same as models for responsible use.
- Users should immediately report misuse or security breaches detected to their department heads and/or to campus ICT managers. Heads of Departments shall address reported breaches or refer these to the ICT Directorate.

## 7.1 Restrictions

The Electronic messaging services should not be used for:

- i. Unlawful activities or those that cause interference with other users;
- ii. Commercial purposes not under the auspices of the University;
- iii. Personal financial gain, except as permitted by the University;
- iv. Personal use inconsistent with Campus and University policies;
- v. Uses that violate other University and Campus policies or guidelines. This includes, but not restricted to policies and guidelines regarding intellectual property, or policies regarding harassment in any form.

# University of Sierra Leone ICT Policy - 2018

---

## 7.2 Misrepresentation

E-mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so.

## 7.3 Personal Use

Although the University's electronic messaging system is meant for university business use, the University shall allow the reasonable use of its electronic messaging systems for personal use if certain guidelines are adhered to:

- i. Personal use of the electronic messaging system should not interfere with work.
- ii. Personal emails must conform to these policies and accompanying guidelines.
- iii. Personal emails are advisedly kept in a separate folder and deleted regularly.
- iv. Users should restrict the number of personal emails sent within working hours.
- v. Mass mailing is not allowed.

## 8.0 Security and Confidentiality

Operators of University electronic mail services are expected to follow sound professional practices in providing for the security of the electronic messaging system under their jurisdiction. Since such professional practices and protections are not foolproof however, the security and confidentiality of electronic mail cannot be guaranteed. Users should therefore be aware that confidentiality may be compromised, by applicability of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. *Consequently, extreme caution should be exercised in using email to communicate confidential or sensitive matters.*

## 8.1 Privacy

- The University reserves the right to monitor **ALL USL** electronic messages and to protect itself from any liability due to the unlawful use of the services provided.
- Further, users should be aware that during the performance of their duties, network and computer operations personnel and system administrators shall periodically observe the performance and operations of transmitting devices to ensure proper functioning of the university e-mail services.

# University of Sierra Leone ICT Policy - 2018

---

## 8.2 Security and Protection

The University attempts to provide e-mail services which are as secure and reliable as practical and as the technology allows. Users are required to assist in the security of their data by employing good password management and usage practices as described in the guidelines accompanying this document.

### 8.2.1 Declaration

- All users should make declaration accepting the terms and conditions governing the use of ICT (See sample in Appendix)

## 9.0 ICT Security

This section is prepared for the direction and use of personnel engaged in the implementation and support of the USL's ICT systems and services delivered thereon. It is intended to inform:

- i. Development and implementation of rules, guidelines and a code of practice to secure the USL's ICT systems and services;
- ii. Development of mechanisms that will help the University to reduce its legal, financial and other risks brought about by an increasingly interconnected world;
- iii. USL community about the rules and practices pertaining to confidentiality and security of the University's ICT resources;
- iv. Custodians of University ICT systems and services about their responsibilities with respect to the preservation of these systems and the sanctions for non-compliance.

### Risk Mitigation:

This applies to the mitigation of the following:

- i. Computer system availability
- ii. Conservation of University ICT assets
- iii. Integrity of University data and information
- iv. The confidentiality of University information
- v. Efficient use of University ICT resources
- vi. The physical security of all computing and communication premises, computers, communication equipment and appliances, transmission paths and computer peripherals.

# University of Sierra Leone ICT Policy - 2018

---

- vii. The physical security of all storage media for data, system software, application software and documentation.
- viii. The physical security of power systems supplying electrical power to network communication and computer systems.
- ix. The logical security of data, information and information processing resources such as databases, computer programs, email records, servers, routers, switches and other network appliances.
- x. Business continuity management

## 10.2 Roles of Campus ICT Services Unit

### The Campus ICT Unit shall:

- i. Account for all ICTs and information resources in their area of jurisdiction that is connected to campus networks by one or other means.
- ii. Provide and maintain a database of all University owned ICT assets.
- iii. Assess the security risk of all ICT systems and apply such security systems and processes as are consistent with the mitigation of this risk.
- iv. Provide and/or commission the physical security of all enterprise servers, databases, backbone network switches and ICT management, teaching and learning platforms.
- v. Advise on the Procurement implement and maintain the logical security systems as are necessary to protect University electronic data and information assets from misuse, damage, loss or unauthorized access.
- vi. Develop, document and publish the ICT security guidelines in accordance with and informed by best practice.
- vii. Promote a security awareness campaign for users of University ICT systems and collaborate with functional departments to design and deliver end user ICT security awareness training.

## 12.0 Physical Security & Integrity of Systems

- Appropriate barriers and controls governing the physical access to and the maintenance of the integrity of critical University ICT assets must be deployed commensurate with the risk identified.

# University of Sierra Leone ICT Policy - 2018

---

- Barriers and controls include, but are not limited to electronic access control to servers and critical network infrastructure, installations of grillwork surrounding and enclosing video systems, fire suppression, and power management systems.
- Physical ICT assets include but not limited to multifunction devices, servers, communication switches, routers, firewalls, personal computers, cameras, printers, plotters, multimedia projectors, media management platforms, scanners, media containing software, books and manuals.
- The physical security and integrity of all ICT resources rest with the ICT Directorate and DVCs of the constituent colleges

## 13.1 Software and Firmware upgrades

- The Directorate must ensure that all computers, switches, routers and other network-attached devices that have the most recent approved and released software and firmware security patches installed as soon as they are generally available.

## 13.2 Malware control

- All computers should have licensed and updated Antivirus software.

## 13.3 Network Interconnections

- All network interconnections shall be guarded, and audited by processes and such perimeter defense and intrusion detection systems, as are appropriate to manage and mitigate identified risks.

## 14.0 Privacy and Confidentiality

- The University requires that the architecture, processes and procedures surrounding software applications must be such that privacy of University data and information is protected.
- Users of University supplied or supported electronic communication system and services must be advised of the procedures required maintaining privacy of University data and information.

# University of Sierra Leone ICT Policy - 2018

---

## 14.1 Right to Monitor ICT Systems

- The University reserves the right to monitor, audit and interdict all electronic payloads traversing its networks or stored on its systems in furtherance of its duty to secure and retain the confidentiality of its data and information resources.

## 15.0 Localized Policies

Campus units may establish or seek to establish complementary policies, standards, guidelines or procedures that refine or extend the provisions of this policy and to meet specific local needs. In any event, such extensions shall comply with University regulations, ordinances and national laws.

## 16.0 Social Media

The term “social media” refers to a set of online tools that supports social interaction among users. Social media has radically changed the way we communicate and interact – both as an institution and as individuals – and offers opportunities to connect and engage with a range of key stakeholder groups including prospective and current students, staff, alumni, donors and friends of the University.

This Policy is intended to assist the USL community to leverage the maximum benefits while mitigating risks of social media networking. This Policy aims to exert positive influence on and help shape the online social behavior of the University community in physical and virtual USL spaces or while using facilities that are owned and/or controlled by USL.

This Policy applies to all USL Social Media Sites and to the activities permitted by these sites. It applies to sites and any activity that falls within the genus of social media, whether they are current or come into existence on or after the date of the approval of this Policy. Examples include weblog posts (blogging), facebook, Twitter, WhatsApp, Instagram, Messenger, snapchat, event updates, news updates, chats, discussion boards/posts, photo/video sharing, music and radio broadcasts and gaming.

# University of Sierra Leone ICT Policy - 2018

---

## 16.1 Definition of Concepts

### **I. Blog**

A contraction of the term “weblog”, which is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

### **II. Competent University Authority**

The Campus ICT Manager or any other person/body performing the function of monitoring and regulating USL Social Media Sites as designated by the Campus Principal or his nominee on the relevant campus. The set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work. These rights can be licensed, transferred and/or assigned.

### **III. Publish/publication**

Any work in whatever form made available to the public at large.

### **IV. Social media**

The set of online tools that supports social interaction between users

### **V. USL Data Network**

Any data network which USL owns, rents, leases or manages, either directly or under a sub-contract.

### **VI. USL Entity**

This refers to any Campus, School, Department, Institute, Unit, Centre, Section, Sub-Section, or other unit of teaching, research or administration of the USL, including any project or programme in which any of them is involved. Bodies such as the Guild of Students, Student Associations, Alumni Association Chapters and entities owned by the USL, for example, USL Consulting Inc. are also USL entities.

### **VII. USL ICT Resources/Systems**

Any Information and Communications assets including but not limited to hardware, software, networking and communications equipment, services and facilities and data and information

# University of Sierra Leone ICT Policy - 2018

---

which are owned, leased or loaned by the USL or its agents irrespective of where these items may be located.

## **VIII. USL Marks**

The USL name, the USL Logo and all other words, logos, signs or marks whether registered or not, that belongs to or associated with USL.

## **IX. USL Social Media Sites**

These are official social media outputs by USL entities acknowledged as representing the University by virtue of recognition by the Competent University Authority.

## **X. USL Spaces**

This refers to any physical, virtual space or facility that is controlled by the USL.

## **XI. USL Staff Member**

A member of the academic, senior administrative, professional, and other non-academic staff, whether permanent or temporary and including staff on sabbatical as well as visiting scholars.

## **XII. USL Student**

A student whether part-time or full-time, registered in any USL course or programme, or with any USL entity/franchise.

## **17.0 General Liability**

- The University of Sierra Leone (USL) shall not be liable for any errors, omissions, loss or damage, including indirect and/or consequential loss and/or damage claimed or incurred due to any use of any ICT resources that does not comply with this Policy or the policies cited herein.

## **18.0 Use of USL Marks**

- Electronic use of USL Marks without permission is illegal. The University Secretariat is the sole agency (headed by the VC & P) from which persons or entities wishing to use USL Marks should seek permission.

# University of Sierra Leone ICT Policy - 2018

---

## 18.1 Compliance with other USL policies

- Information published on the internet should conform to all applicable USL policies
- Content posted by USL members shall conform to the University's principles of confidentiality and information disclosure which are included in the relevant Codes and Principles of Ethics for both staff and students.

## 18.2 Penalties for Misuse

Where there is evidence of misuse of ICT resources, the USL may restrict or prohibit the use of its ICT resources and/or, where appropriate, request external entities to take action against offenders. USL members who breach this Policy may face disciplinary action up to and including termination of employment in the case of staff members; and suspension or expulsion in the case of students.

# University of Sierra Leone ICT Policy - 2018

---

## Annexes

### Annexes I

#### User Acceptance

I understand that the USL provides, operates and maintains its ICT resources to support its instructional, research, and administrative activities.

I understand that my assigned access credentials (including user names, passwords, access cards, biometric features and PINs) identify and allow my access to the USL's ICT resources and that I am accountable for the protection of my access credentials. I also accept that I am responsible for all actions committed through the use of my access credentials.

I understand the USL has the right to access, impound and search any of its ICT resources at any time and for any reason, including determining compliance with University, Campus or other information security requirements.

I will comply with the USL's Acceptable Use Policy and accept that as a user of the USL's ICT resources I have a responsibility for the security of those resources. To the best of my ability I will protect the USL's ICT resources from unauthorized use, modification, destruction or disclosure, whether accidental or intentional. I agree to be bound by the current version of the USL's Acceptable Use Policy, which will be freely available to the University community.

I understand that abuse of these requirements, and others which may be declared in the future, may result in disciplinary and/or legal action.

I hereby acknowledge that I have read and understand the USL's Acceptable Use Policy and this User Acceptance of Security Responsibility and agree to be bound by the conditions herein.

Name:	Date:
Signature:	Student/Staff ID No:
Position: Campus:	Office/Faculty:
Department/Unit:	

# University of Sierra Leone ICT Policy - 2018

---

All users of the ICT resources of the USL are required to sign the above document, or otherwise signify acceptance of this policy, and thereby commit to abide by its provisions. This document covers the ICT resources of the University of the Sierra Leone, which include, but are not limited to:

- i. Hardware;
- ii. Software;
- iii. Networking equipment, services and facilities;
- iv. Learning and teaching platforms and systems;
- v. Communication equipment, services and facilities;
- vi. Data and information.

## Annex II

### Declaration

I have read, understood and now acknowledge receipt of the E-mail policy. I will comply with the provisions of, and accompanying guidelines to, this policy; and understand that failure to do so might result in disciplinary or legal action being taken against me by the University of the Sierra Leone

Signature: Date:

Printed Name:

Campus/Department/Faculty/Unit:

# University of Sierra Leone ICT Policy - 2018

---

## **Bibliography**

Durham University – Policies A - Z 2018

The University of Makerere Policies 2018

The University of Ibadan 2018