MSRUAS ICT Policy

RAMAIAH UNIVERSITY OF APPLIED SCIENCES

Chief Manager - ICT
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054.

Registrar
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054

M. S. Ramaiah University of Applied Sciences
University House, New BEL Road, MSR Nagar, Bangalore – 560 054
www.msruas.ac.in

Contents

e. take disciplinary action if users have been found to be indulging in any illegal or unacceptable use of the ICT Resources including:
    i. wilful physical damage to any of the ICT Resources;
    ii. improper access to confidential information;
    iii. destruction or deliberate interruption of information or the free usage of other resources;
    iv. disseminating information without appropriate permissions;
    v. engaging in malicious activities including unauthorised access to user accounts and passwords;

8. Reasonable Personal Use:

   Users may be permitted to use the ICT Resources for limited, incidental purposes. Such use must not impose significant additional costs to the University. Examples of permitted personal use are online banking, travel bookings, browsing for permitted purposes etc.

   Reasonable use in the context of the particular circumstances is a matter to be determined by the User's Head of Department or Administrative Head. The University's decision in this regard shall be final.

9. Consequences of Breach of Policy:

   Users found to have breached this Policy will be subject to disciplinary action in accordance with the University's disciplinary procedures and could result in the imposition of fines, recovery of damages and/or costs or even imprisonment. Criminal offences will be reported to the law enforcement authorities.

   The University will not defend or support any user who uses the ICT resources for an unlawful purpose.

   Where a user is not a member of the University and is found to have breached this Policy such users may be subject to action as deemed appropriate by the University. If the action is criminal in nature it may be reported to the law enforcement officials for action.

10. University Course and Other Materials:

    Authorised users of the University should ensure that all course materials are placed on the University's servers and not on personal web pages or servers. They are required to observe University policies and procedures failing which they will be liable to disciplinary action.

11. University Liability:

    The University accepts no liability or responsibility for any loss or damage whether direct or consequential arising from the personal use of the ICT Resources.

1.6 Access for Mobile Computing Devices

Mobile computing devices include notebooks, handheld devices, other peripheral devices (including printers, disk drives, monitors, keyboards, mice etc.) and associated software.

Mobile computing devices given by the University to authorized users are the responsibility of the user. These devices must be returned to the University on demand or on employee's departure.

Users are required to exercise sufficient care in ensuring that unauthorized persons do not have access to mobile computing devices and to keep information on such devices fully confidential. Passwords should be implemented on such devices to prevent unauthorized access.

Mobile computing devices may be provided access to the University's network only at designated points or locations.

1.7 Email & Messaging

All University E-mail IDs will adhere to the format defined below. No other formats will be supported by the University.

Employee Email ID format

Sl. No.	Category of Employees	Format	Email ID (example)
1.	University Officers	Designation@msruas.ac.in	vc@msruas.ac.in pvc1@msruas.ac.in pvc2@msrsuas.ac.in registrar@msruas.ac.in director-admissions@msruas.ac.in registrar.acad@msruas.ac.in
2.	Faculties		
	Officers	designation.facultycode@msruas.ac.in	dean.et@msruas.ac.in dean.ad@msruas.ac.in dean.mc@msruas.ac.in registrar.acad.et@msruas.ac.in registrar.admin.et@msruas.ac.in
	HODs	designation.departmentcode.facultycode@msruas.ac.in	hod.me.et@msruas.ac.in hod.ee.et@msruas.ac.in
	Academic Faculty Members and other members of the department	name.departmentcode.facultycode@msruas.ac.in	anilkumar.me.et@msruas.ac.in nmurthy.cs.et@msruas.ac.in
	Administrative Managers	Designation.centrecode.facultycode@msruas.ac.in	manager.e1.et@msruas.ac.in manager.a1.et@msruas.ac.in manager.e2.ad@msruas.ac.in manager.a2.ad@msruas.ac.in

Student Email-ID format

Student name with last 3digits of registration number .departmentcode.facultycode@msruas.ac.in

Example:

anilkumar001.me.et@msruas.ac.in

The University owns all copyrights to email correspondence created by members of its staff in relation to their employment duties.

When using the email or messaging systems Users are responsible, at all times:

a) To respect the privacy and personal rights of others;
b) To take all reasonable steps to ensure that no copyrights or IPR are infringed;
c) Not to forward emails containing any personal information;
d) Not to send sexually explicit or other inappropriate material;
e) Not to send SPAM (unsolicited e-mails);
f) Not to harass, threaten or intimidate other persons or users;
g) Not to send forged messages, forward viruses or other attachments, bulk messages and the like;
h) To ensure that appropriate standards of civility are observed when using email and messaging services, i.e., no angry or threatening messages, offensive, intimidating or humiliating messages may be sent using the ICT Resources;
i) To ensure that care is exercised to refrain from forwarding or copying from any web pages material that is protected by copyright whether it is an audio, video file, music, photographs or text.

1.8 Desktop Environment

The University will endeavor to implement a standardized desktop environment for all locations to ensure that ICT Department staff can resolve issues efficiently and quickly. The standardized environment will provide users a similar look and feel, uniform access to computer equipment and software applications across the University, support remote access to systems by ICT personnel and users and better maintenance by ICT personnel.

Users must not change or delete any settings that have been made by ICT Department on desktops or other devices. These include Network settings, control panel settings, Icons on the desktop, password settings etc. Users are also required to use passwords and change passwords at regular intervals and to shutdown computers etc. using proper procedures.

1.9 Access to the Internet

The ICT Department will provide users with appropriate access to the Internet to perform their functions properly. Users shall abide by the University's policies in this regard.

a) Users shall use the internet only for approved purposes. Improper usage may result in immediate termination of access.
b) Usage may be monitored by ICT Department for any unusual or inappropriate activity. ICT Department's decision in relation to the provision or termination of services to any user shall be final in all matters.

c) Users should respect all copyright laws and other licensing agreements. Failure to do so may result in loss of access privileges and/or penalties.
d) Users will abide by the Acceptable Use Policy of the University.
e) Users shall not:
    i. visit internet sites that contain obscene or other objectionable material;
    ii. Use the internet or email services for illegal purposes, gambling, playing games, commercial purposes.
    iii. Post offensive remarks, comments, indecent material;
    iv. Download any software or other electronic files without using virus protection and/or filters approved by the University;
    v. Use internet access during office hours on non-University affairs;
    vi. Upload, download or transmit copyrighted material;
    vii. Perform any other inappropriate use prohibited by the ICT Staff.
f) Users who violate any of the above guidelines will be subject to disciplinary action by the University.
g) In the case of gross misuse or misconduct access will be terminated immediately and in the case of an employee dismissal procedures will be initiated.
h) All employees and students will be required to sign an undertaking, included in their employment contract, agreeing to abide by the University's policies and procedures for accessing the using the ICT Resources, email and internet services.

1.10 Security, Privacy and Compliance

1.10.1Security & Privacy

a) Matters of a confidential nature shall only be conveyed or stored in an electronic format when adequate security measures have been taken.
b) While the University communications systems are electronically safeguarded and maintained in accordance with current best practice, no guarantee can be given regarding the protection confidentiality, privacy or security of any information.
c) Email and other records stored in ICT Resources may be the subject of a search warrant, discovery order or application under criminal activity. Disclosure outside the University any personal information, irrespective of its format, shall be considered as breach of information and shall be dealt appropriately.
d) The University may collect and receive personal information of Users and others in the course of managing the operation and use of its ICT Resources and that information can be used in connection with efforts to ensure that Users comply with all relevant laws and University policies.
e) Communications on University business in any format or media are official records, subject to statutory record keeping requirements and the University Record keeping Policy. This shall include email sent and received by staff members on any University related matter. Staff members need to be conscious of the need to preserve official communications in accordance with the relevant University guidelines on the management of electronic records. Care should be

taken before deleting any electronic communication that it is not required to be kept as evidence of a decision, authorisation or action.

f) Sending an email on an official University matter shall be considered similar to sending a letter on University letter head. Such email transactions shall have to be handled with the normal courtesy, discretion and formality of all other University communications. Users shall not write anything in an email that they would not sign off in a memorandum.

g) All accounts, data, files, email messages of Users are stored on the ICT Resources of the University and are normally held private and secure from access by other users. However there may be situations such as repairing, upgrading or restoring servers etc. when properly authorised staff of the University may be required to:

   i. Access user accounts;
   ii. Temporarily suspend access to accounts;
   iii. Disconnect computers and/or other ICT resources from the University's network;

1.10.2Access & Physical Control

a) New Users will be allocated Usernames and Passwords by ICT Department for all systems.

b) The level of access provided to Users will be based on their need.

c) Users will be provided with the required User Documentation for all systems maintained by the ICT Department.

d) Appropriate barriers and controls governing the physical access to, and the maintenance of, the integrity of University ICT assets shall be deployed commensurate with the risk identified. Such risks include identified natural and environmental hazards.

e) 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. Authentication and authorization functions shall be employed for all users of University electronic data and information resources. A central authentication database shall be established for all users. Procedures to manage access, authentication and authorization shall be developed to support and manage these activities. Such processes and procedures shall include but shall not be limited to user passwords for network and application access, biometric access mechanism, tokens and electronic key devices.

f) ***Software and Firmware upgrades:*** All computers, switches, routers and other network-attached devices shall have the most recent approved and released software and firmware security patches installed as soon as they are generally available.

g) ***Virus Protection:*** University approved virus protection software must be installed on all devices on the network. Such software must be regularly updated and scanned for viruses regularly.

h) ***Malware control:*** Malware is a common feature of globally connected networks. Personnel engaged in the implementation and support of the University's ICT systems shall take all appropriate steps to protect its ICT assets from damage, compromise or loss of confidentiality. For the purposes of this policy, malware is defined as software agents that by their action deny users the maximum capabilities of the ICT systems, compromise the security and confidentiality of university data and information or destroy or damage university ICT assets. Malware include but is not limited to spyware, viruses, worms and spam.

i) ***Network Interconnections:*** Interconnections among networks are unavoidable in the ordinary course of business. These interconnections are portals for unauthorized access and entry to University networks and pose significant risk to the security of University data and information resources. Therefore all network interconnections shall be guarded, and audited by processes and such perimeter defence and intrusion detection systems, as are appropriate to manage and mitigate these risks.

j) ***Access to Business Critical systems:*** The University is dependent on several of its major systems for its daily operations. Breaches to their integrity, or their unavailability for any significant period of time, could reduce the service delivery capability or place the institution in disrepute. Such systems may include the Student Administration System, online teaching and learning platforms, the financial management system, the enterprise planning and/or human resource management information system. Notwithstanding the general security safeguards enunciated before, these business-critical systems shall be provided with an elevated level of security. These additional measures shall include, but are not limited to, internal firewalls, secondary access challenges and biometric access controls. When the security requirements are stringent enough, internal isolation of the network segment to which such systems are attached is the final consideration.

1.11 Monitoring

The University reserves the right to monitor files, data, server logs, websites and e-mails stored on or accessed using the ICT Resources and network of the University and to access any other device that may be connected to the University network including personal computing equipment like laptops. The University reserves the rights to monitor the use of its ICT resources to ensure compliance with this policy.

1.12 Response to Breaches

1. The University reserves the right to withdraw, restrict or limit any User's access to its ICT Resources if a breach of these conditions 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.
2. Further the University 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.

1.13 Data Backup Procedures

Users should follow the procedures laid down below as far as possible:

1.13.1File Naming Conventions

File names should indicate the content of the data within it especially where the files are shared with many users.

1.13.2Directory/Folder Naming Conventions

Registrar
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054

Chief Manager - ICT
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054.

The users shall be required to comply with the guidelines prescribed in this regard from time to time.

1.13.3Application Directories/Folders

Staff installing applications should use the Default Directories for all applications installed.
Where "default directory locations" are not provided the installer must choose the most obvious directory name for installing the application.

1.13.4Backup Procedures

All Users are individually responsible to ensure that their information and data is effectively backed up. The University does not accept any responsibility for the loss of data or information held on University ICT Resources or User's personal resources connected to University ICT resources.
Where several users are accessing/using one computer one person should be nominated with the responsibility of actively monitoring the backup procedures for all information accessed by that group.
Backup logs should be maintained by Users.
All Backups should be appropriately labelled and date indicated clearly.
Backups should be stored in a safe, secure and off-site location.

1.14 Hardware & Software Acquisition & Maintenance

- Hardware & Software procurements:
  i. All requirements of hardware/software should be forwarded to the ICT Department and should be supported with a "Hardware/Software Requisition Form" from the Requisitioning Department together with the justification for the request and duly approved by the relevant authority.
  ii. Hardware/Software requests should, as far as possible, conform to the standard configuration, system and application software standards laid down by the University.
  iii. The ICT Department may or may not proceed to procure the hardware/software item requested or may make modifications to the configuration to conform to University norms.
  iv. All hardware/software purchased should be compatible with the result of the University's computer equipment.
- Copyrights:
  Users should be aware of and abide by the University's policy on copying and using computer software that are protected by copyright and other licenses and laws or contractual agreements with vendors.

1.15 Web Publishing Guidelines:

The University's **Publications & Outreach Committee** is responsible for:

- ensuring that the standards of publication are continuously monitored;
- resolving all issues relating to the appropriateness of material published on the University's website.