ACCEPTABLE USE OF COMPUTERS AND NETWORKS

PURPOSE AND SUMMARY

Vijayanagara Srikrishnadevaraya University ("VSKU" or "the University") provides computing and networking resources to all qualified members of the University community. Access to computers, computing systems, and networks owned by the University is a privilege which imposes certain responsibilities and obligations and which is granted subject to University policies and codes, and Local, State, and Central Government laws. All users of these resources must comply with specific policies and guidelines governing their use, and act responsibly while using shared computing and network resources, including wireless.

This policy applies to all users of the University's computing and network resources, whether initiated from a computer and/or network device located on or off campus.

"Antivirus Software" is software specifically designed for the detection and prevention of known computer viruses.

"Spam" is unsolicited junk e-mail sent to large numbers of people to promote products or services.

Acceptable Use Guidelines

1. Users shall take no actions that violate the Codes of Conduct and Academic Integrity, or other applicable policy or law.
2. Users shall take security measures to protect the integrity of information, data, and systems. Users shall protect their computer systems and accounts by using strong passwords; installing “Antivirus Software” consistent with management directives; and

keeping such software, as well as the operating system and application security patches, up to date.

3. Users are responsible for safeguarding their identification codes and passwords, and for using them only as authorized.
4. Users shall use the computer and network resources efficiently. Computing resources are finite and must be shared.
5. Users may use the University's computer and network resources for incidental personal purposes, provided that such use does not (a) unreasonably interfere with the use of computing and network resources by other users, or with the University's operation of computing and network resources; (b) interfere with the user's employment or other obligations to the University; or (c) violate this policy or other applicable policy or law.
6. The University retains the right to set priorities on use of the system, and to limit recreational or personal uses when such uses could reasonably be expected to cause, directly or indirectly, strain on any computing facilities; to interfere with research, instructional, or administrative computing requirements; or to violate applicable policies or laws. Examples of inappropriate use include circumventing the editor or moderator to post messages to private (closed) listservs, sending "chain letters" or engaging in pyramid schemes, or engaging in unauthorized peer-to-peer file sharing. Sending "spam" or posting inappropriate promotional or commercial messages to discussion groups or bulletin boards, is not permitted.

Misuse of University Assets

7. Users shall not harass or intimidate or use computer and network resources for unlawful acts. The University, in general, cannot and does not wish to be the arbiter of content

maintained, distributed, or displayed by users of the University's computing and network resources. For example, the University, in general, cannot protect users from receiving e-mail they may find offensive.

8. Using the University's computer or network resources for illegal activities, however, is strictly prohibited. Unlawful use of University computer and network resources can expose the individual user to damages claims and/or potential criminal liability. Unlawful uses may include, but are not limited to, harassment and intimidation of individuals on the basis of race, sex, religion, ethnicity, sexual orientation, or disability; obscenity; child pornography; threats; theft; attempting unauthorized access to data; attempting to breach security measures on any electronic communications software or system; attempting to intercept electronic communication transmissions without proper authority; and violation of intellectual property or defamation laws.

9. Users shall not use computer systems to send, post, or display slanderous or defamatory messages, text, graphics, or images. By using the University's computer and network services, each user accepts the responsibility to become informed about, and to comply with, all applicable laws and policies.

10. The use of University computer resources and networks is for legitimate academic or administrative purposes. Incidental personal use is permissible to the extent that it does not violate other provisions of this policy, interfere with the performance of the employee's duties, or interfere with the education of students at the University.

11. Use of computer account or the network for commercial activities that are not approved by appropriate supervisory University personnel consistent with applicable policy, or for personal financial gain (except as permitted under applicable academic policies) is

prohibited. Examples of prohibited uses include using the computer account for engaging in unauthorized consulting services, software development, advertising products/services, and/or other private commercial activity.

12. Misuse of University property includes, but is not limited to, stealing or damaging equipment or software, knowingly running or installing computer viruses or password-cracking programs, attempting to circumvent installed data protection methods that are designed and constructed to provide secure data and information, in any way attempting to interfere with the physical computer network/hardware, or attempting to degrade the performance or integrity of any campus network or computer system.

13. Authorized University personnel (e.g., system, network, and database administrators, among others) may have access to data beyond what is generally available. Privileged access to data may only be used in a way consistent with applicable laws, University policies, and accepted standards of professional conduct. Those who have access to databases that include personal information shall respect individual privacy and confidentiality, consistent with applicable laws and University policies regarding the collection, use, and disclosure of personal information.

14. Users should be aware however that state laws and University policies, guidelines, and regulations may prevent the protection of certain aspects of individual privacy. Both the nature of electronic communications and the public character of the University's business make certain uses less private than users may anticipate. For example, in certain circumstances, the University may permit the inspection, monitoring, or disclosure of e-mail, consistent with applicable laws and with the University's Electronic Mail Policy.

15. Users when using a University computer system and/or network to connect to a non-VSKU system or network, shall adhere to the prevailing policies governing that system or network. This does not in any way release the users obligation to abide by the established policies governing the use of VSKU's computer systems and networks.

Recourse for Misuse and/or Noncompliance

Aforementioned policies in this document include action steps to be taken to determine whether or not an individual has, in fact, misused University computing and/or network resources. Protections of the rights of individuals accused of policy violations afforded by those policies also apply.

Users who misuse University computing and network resources or who fail to comply with the University's written usage policies, regulations, and guidelines are subject to one or more of the following consequences:

- Temporary deactivation of computer/network access
- Permanent deactivation of computer/network access
- Disciplinary actions taken by the department or Dean of Students Office up to and including expulsion from school or termination of employment
- Subpoena of data files
- Legal prosecution under applicable Central and state laws
- Possible penalties under the law, including fines and imprisonment

Prohibited use

- Supporting, establishing, or conducting any private business operation or commercial activity not expressly allowed by VSKU policy.
- Engaging in political activities that violate State or Central laws.
- Conducting personal activities unrelated to any VSKU or student educational purpose unless otherwise allowed by the University policy, including harvesting VSKU e-mail addresses for personal use.
- Attempting to gain unauthorized access to any portion of the VSKU computer system or using VSKU IT resources as a staging area to attempt to gain unauthorized access to any other system or account.
- Violating VSKU's policy of prohibiting discrimination against individuals on the basis of caste, sex (including sexual harassment), religion, age, color, creed, national or ethnic origin, physical, mental, or sensory disability, marital status, sexual orientation or the use of a trained service animal by a person with a disability.
- Intentionally disseminating, accessing, or providing a hyperlink to obscenity, as that term is defined by the law, unless such activities are directly related to an employee's legitimate research or scholarship purpose or to a student's completion of an academic requirement.
- Sending unsolicited electronic mail (e.g., "spam").
- Destroying, altering, or compromising the security, privacy, integrity, or availability of IT resources when such uses are not authorized.
- Utilizing VSKU systems to intentionally interfere with others' use of IT resources or conduct of VSKU business;

- Violating copyright law (thus, information technology and network users who do not hold the copyright on a work must have permission to publish information, graphics, cartoons, photographs, or other material, or the publication must be otherwise permitted under copyright law); or Violating trademark law, Export Control law, or other Central, State, or local law, or VSKU policy.

Maintenance and management of accounts

- Email is provided for academic and other official communication purposes only.
- Email accounts shall remain in possession of the employee/staff/student until he/she is associated with the university. Up on separation from the university the account shall be terminated and user data shall be deleted.
- The University does not maintain any backup of the data contained in the email/ user accounts. Users are encouraged to maintain a backup of all their data as and when necessary.
- The University shall not be liable for any loss of user's data anytime during operation of the accounts.
- Users shall not store any material that is illegal or declared prohibited by the University, on the University's storage systems. Any user in such a violation shall be subject to disciplinary action according to the University's regulations and/or appropriate legal punitive actions according to Local or State or Central governmental laws.
- Data storage may be monitored for inappropriate items such as photos and/or movies that are not academically relevant. Any such items, if found, shall be deleted without any notification and appropriate disciplinary proceedings shall be initiated against the user.

- Any files that are unreasonably large in size may not be stored on the University's storage systems unless authorized by the University's ICT Department.

ELECTRONIC CORRESPONDENCE

Electronic correspondence shall be one of the authorized means of communication from the University to students, faculty, staff, and other constituents.

Electronic correspondence includes both traditional two-way or multi-way communications between or among correspondents (i.e., individuals, businesses, agencies) and official, one-way, targeted messages, announcements, or other forms of communication from the University.

Any confidential or Individually-identifiable information must not be sent electronically and must be sent and delivered by secure means.

Originator Responsibility

University electronic correspondence may be used only to meet academic instruction, research, public service, and administrative needs of the University. Originators are responsible for selecting the appropriate correspondence mechanism. Delivery-tracking mechanisms should be used when necessary to ensure legal or business procedure compliance.

Recipient Responsibility

Faculty, staff, and students are responsible for all information sent to them via University-provided electronic correspondence delivery mechanisms. The University expects that all University business-related electronic correspondence received will be read in a timely fashion, and without the need for follow-up notices.