SRI DEVARAJ URS ACADEMY OF HIGHER EDUCATION AND RESEARCH

A Deemed to be University
Tamaka, Kolar, Karnataka.

Declared under Section 3 of the UGC Act, 1956
vide MHRD, Government of India Notification
No.F-9-36/2006-U.3 (A) dated 25th May 2007

KNOWLEDGE FOR POSTERITY

SDUAHER

SOCIAL MEDIA POLICY

SRI DEVARAJ URS ACADEMY OF HIGHER EDUCATION & RESEARCH

A DEEMED TO BE UNIVERSITY, (DECLARED UNDER SECTION 3 OF THE UGC ACT, 1956)

TAMAKA, KOLAR 563101, KARNATAKA, INDIA

Name of the Policy/ Guidelines	Social Media Policy	
Short Description	The policy provides SOP for proper usage of social media	
Scope	The policy is applicable to all faculty and non-teaching staff of the constituent colleges and departments of SDUAHER (Deemed to be University).	
Policy status	☑ Original □ Revised	
Date of approval of Version 1	**14 October 2020**	
Policy No.	SDUAHER/KLR/POLICY/024	
Brief description of last revision	Not Applicable	
Date of approval of current revision	Not Applicable	
Effective date		
Approval Authority	Board of Management	
Responsible officer	Registrar	
Name of the Policy/ Guidelines	Policy and guidelines on welfare measures applicable to teaching and non-teaching staff	
Details of Revision	Date of Revision	Approved by

Social Media Policy

1.0 Introduction

Social media includes all means of communicating or posting information or content of any sort on the Internet, including own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, as well as any other form of electronic communication whether or not associated or affiliated with the University that is Sri Devaraj Urs Academy of Higher Education and Research (SDUAHER).

As Social Media has become an intrinsic part of everybody's life, it is extremely pertinent to maintain a clear demarcation between one's personal vis-a-vis professional presence on social media so as to ensure that work ethics are upheld. An employee remains solely responsible for what is posted by him/her online. Before creating online content an employee should keep in mind that any such conduct can adversely affect his/her job performance, the performance of fellow associates or can adversely affect the reputation of the institution. Patient clientele, students, vendors, or legitimate interests of the SDUAHER management can also be affected adversely as a consequence of such an act.

It should be understood by all employees that, other members of social media who are aware of an employee's association with SDUAHER, are likely to associate an employee's conduct on social media with that of SDUAHER.

2.0 Purpose of Social Media Policy

This policy is being laid down with the intention to promote good practice so as to mitigate the risks related to wrongful use of social media which can impact the wellbeing of the University (meaning SDUAHER and its affiliate units viz. SDUMC, RLJH & RC, its students, teaching faculty members, staff, patient clientele and other stake holders) and its reputation. This policy would serve the under mentioned purpose:

a) To promote effective and innovative use of social media as part of the Academy’s activities.

b) To disseminate information to all concerned about the duties and responsibilities regarding the use of social networking platforms.

c) To create awareness regarding penal actions that can be initiated against a defaulting employee for breach of Social Media Policy.

3.0 Applicability of the Policy

a) This policy relates to all employees (viz. Permanent, Probationary, Temporary and Contractual) who create or contribute to blogs, wikis, social networks, apps, forums, virtual worlds, or any other form of electronic communication using social media. It shall be applied to use of all types and forms of use of social media where there is a potential impact on the Academy viz. whether work-related or personal use, whether used during working hours or otherwise, whether social media is accessed using the Academy’s IT facilities and equipment, or equipment belonging to other employee(s) or any other third party.

b) Third parties who have access to the Academy’s electronic communication systems and equipment are also required to comply with this policy.

4.0 Policy Guidelines

4.1Employees, while on social media, should not normally discuss anything about the workplace related activities. If, however, it becomes necessary, the employees shall restrict their comments within the limits of their own area of expertise to provide individual perspectives on non-confidential activities at the Academy.

4.2 Employees should never represent themselves or the Academy in a false or misleading way.

4.3 Employees should use common sense and common courtesy. They should ask permission to publish or report conversations that are meant to be private or internal to the Academy.

4.4 The Academy's guidelines for external communication should not be violated by an employee's efforts to be transparent.

4.5 Where employees access social media for work-related purposes or personal use using the Academy's IT facilities and equipment, the Academy's IT regulations will apply.

4.6 Where ever appropriate, the Academy reserves the right to monitor the use of social media platforms and take appropriate action(s) to protect itself against any misuse that may be harmful, in accordance with the IT regulations and where the law permits.

4.7 Employees should seek guidance before participating in social media when the topic being discussed may be considered sensitive (e.g. a crisis situation, intellectual property, issues which may impact on the Academy's reputation, any sensitive issue for that matter). Social media activities related to sensitive topics should be referred to the Director, MACC immediately on being noticed by any employee.

4.8 If an employee's use of social media is considered to be derogatory, discriminatory, bullying, threatening, defamatory, offensive, intimidating, insulting, harassing, creating legal liability for the Academy, bringing the Academy into disrepute, breaching the provisions of this policy or any other policy / procedure of this Academy, then the

Academy may initiate disciplinary action as per the service rules. Such violations may include posting of comments, videos, or photographs on social media sites about the Academy, students, colleagues or office bearers.

4.9 An employee should not engage in any illegal activity through social media or engage in any activity that promotes terrorism, unrest, religious disharmony, hatred or treason. The very act of possessing, disseminating or posting material(s) related to terrorism, secessionism may be sufficient to warrant an investigation by the law enforcing agencies.

4.10 The Academy's response to any misuse of social media by an employee in a personal capacity shall be reasonable and proportionate to the perceived offence, the nature of the postings/comments made and the impact or potential impact on to the Academy.

4.11 Social networking sites may be referred to when investigating misconduct.

4.12 Employees should be aware of cyber security threats and be on guard for social engineering and phising attempts. It is important to be aware that social networks can also be used to distribute spam and malware.

4.13 The Academy may call upon employee(s) to remove social media postings which are deemed to constitute a breach of this policy and any failure to comply with such a request may, in itself, result in disciplinary action.

4.14 An employee has to be always honest and accurate when posting information or news, and in case a mistake has been done, the same has to be corrected at once. No employee should post any information or rumors about the Academy, fellow associates, members, any stakeholders or other institutions that is unverified or false.

4.15 No link should be created by any employee from his/her blog, website or other social networking site(s) to Academy website without being authorized in writing to do so.

4.16 Employees shall refrain from using social media while on work or use equipment provided by the institution, unless it is work-related and authorized by any superior official.

4.17 E-mail addresses of the academy or its affiliated offices/officers should not be used to post any material on social networks, blogs or other online tools utilized for personal use.

4.18 No employee should speak or communicate to the media, print or electronic, on behalf of the Academy without any explicit authorization to do so. All media inquiries should be directed to the person(s) authorized by the Academy or its affiliated institutions to interact with the media.

4.19 On noticing any content in social media that disparages or reflects poorly on the Academy, it’s employees or it’s stakeholders, an employee should contact his/her Head of Department or the Head of MACC/IT Section and report the same. Each staff is responsible for protecting the reputation of the Academy. MACC/IT section would immediately swing into action to investigate the incident and promptly delete such content.

4.20 Employees should use institutional e-mail address(es) for the conduct of business (read correspondence) of the Academy via social media. Use of private e-mail addresses for business of the Academy is prohibited.

4.21 Staff should not do anything which endanger or compromise the confidential information and intellectual property of the Academy through the use of social media.

4.22 In addition, staff should avoid misappropriating or infringing the intellectual property of other organizations and individuals, which might have a damaging potential for the Academy, as well as any individual author/research worker.

Staff must not use the logo, brand name, slogan or other trademark of the Academy or it's constituent/affiliated units in any social media post.

5.0 Personal use of social media

The Academy recognizes that employees may work long hours and may occasionally desire to use social media for personal activities at work or by using the computers of the Academy, networks and other IT resources and communications systems. The Academy permits such occasional use so long such activities do not involve unprofessional or inappropriate content and at the same time do not interfere with employment responsibilities or productivity. While using social media at work, circulating chain letters or other spam is never permitted. Circulating or posting commercial, personal, religious, antinational, terrorist or political solicitations, or promotion of outside organizations unrelated to the affairs of the Academy are strictly forbidden.

6.0 Non-compliance to this policy

Any incident of non-compliance to this policy is liable to invite disciplinary actions including dismissal. Disciplinary action may be taken regardless of the fact whether the breach was committed during working hours, and regardless of whether the equipment or facilities of the Academy have been used for the purpose of committing such a breach.

Any employee suspected of committing a breach of this policy will be required to co-operate with the investigation initiated by the Academy or statutory bodies which may involve handing over relevant passwords and login details. The Academy also reserves the right to suspend internet access where it deems necessary during a process of investigation.

7.0 Monitoring

The contents of the IT resources and communications systems of the Academy are it’s property. Therefore, employees using such resources should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media chats/posts/conversation/message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on the electronic information and communications systems of the Academy.

The Academy reserves the right to monitor, intercept and review, without any prior notice, activities of the employees using its IT resources and communication systems, including but not limited to social media postings and activities, to the extent permitted or as required by law, to ensure that the Academy’s rules are being complied with for legitimate purposes and it’s employees meet the terms to such monitoring while they use such resources of the Academy.

This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The Academy may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without prior notice.

Staff should not use the Academy’s IT resources and communications systems for any matter that they wish to keep private or confidential from the College.

8.0 Personnel responsible for implementing the policy

The overall responsibility for the effective operation of this policy is delegated to the Head of IT Infrastructure Services. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimize risks also lies with the Head of IT Infrastructure Services.

9.0 Review of this policy

The Academy shall reserve the rights to review this policy to ensure that it meets legal requirements and reflects best practice.