Policies & Procedures Manual
Sir Syed University of Engineering & Technology

Title of Policy: Social Media Policy and Procedure	
Revision Date (if any): 16-10-2020	
Policy Area: Social Media	**Policy Number: SSUET/P/Gen/022-V2**
Approved by (Statutory Body/ Competent Authority): BOG # 61.7	
Approval Date: 10-10-2020	**Effective Date: 10-10-2020**
Date of Issue: 10-10-2020	
Total Pages: 15	

Policy Statement
It is the policy of SSUET to establish a quality management system that meets the quality standards expected by its stakeholders. To achieve this, SSUET management is committed to continuous improvement in all areas of activities.

	Name	**Designation**	**Date**
Prepared by:	**Mr. Saqib Jawaid**	**Hon. Consultant Cyber Security**	**01-06-2020**
Reviewed by:	**IT Steering Committee**		**16-10-2020**

Table of Contents

Social Media Policy & Procedure

1 Preamble

The social media policy and procedure version 1 was approved in 61th BOG (item number 61.7) on 10-10-2020. On the advice of legal advisor of SSUET some modifications were made in version 1 which are written in this document as version 2.

2 Introduction

Cyber citizenship refers to what it means to be a participant in the online or cyber community or be a user of information networks and their resources. The privilege of accessing and using SSUET's information resources, systems, and networks includes certain responsibilities and obligations. It is subject to University policy and the laws and regulations of the nation. It is also subject to a set of core University values that honour principals of ethics, academic integrity, academic freedom, and other community standards.

2.1 Purpose and Scope

This policy describes the rights, privileges, responsibilities, and obligations of the SSUET community with respect to the use of SSUET's network and its information resources and services (whether owned by SSUET or provided via SSUET's relationship with a third party) and concerning participation in the cyber community of the Internet. It is the overarching SSUET policy for cyber citizenship. Unit-level policies, procedures, guidelines, and agreements must be consistent with the tenets of this policy; units may supplement, but not relax nor contradict, the restrictions, responsibilities, and obligations established herein.

The policy applies to all faculty and staff members and all university students, individually or as groups where appropriate. It also applies to all others to whom access to the SSUET network or information resources and services is granted.

3 Policy

SSUET's network and its information resources and services (hereafter referred to as SSUET information systems) serve the University's education and research missions and facilitate its business functions. Individuals and groups are granted access to SSUET information systems to further those purposes.

The remainder of this policy describes, in general terms, who may be authorized to use SSUET information systems and what latitude those authorized may have, again in general terms, as to what are and what are not permitted activities. Conditions of Use and similar policy statements may further restrict what may be allowed for specific SSUET information systems.

Information technology and its use are ever-evolving, so no policy such as this can anticipate every possible contingency, nuance, or future development. Instead, this policy will rely on general principles of ethical behaviour and good citizenship in its

application to unanticipated situations. Director IT has the authority to adjudicate disputes in the interpretation of this policy.

4 Appropriate Use and Authorized Users

Appropriate use should always be ethical, reflect academic integrity and other community standards, show restraint in the consumption of shared resources, and comply with SSUET's policies and government laws and regulations. It should demonstrate respect for intellectual property, ownership of data; system security mechanisms; and individuals' rights to privacy and freedom from intimidation, discrimination, harassment, and unwarranted annoyance. Appropriate use of SSUET information systems includes instruction, independent study, authorized research, independent research, communication, and official work of the offices, units, recognized student and campus organizations, and agencies of the University.

Appropriate use may be further defined by Conditions of Use or similar statements for specific elements of SSUET information systems. Who may be authorized to use SSUET information systems depends on the characteristics and purpose of the resource or service. Some, by their very nature, are intended for use by anyone without specific authorization (such as the SSUET web site). Others (e.g., SSUET's email service) are provided to all the members of the SSUET community (faculty, staff, and students). In contrast, others are still restricted to a specific subset of the community (for example, a departmental file server).

The Director IT is vested with the overall authority to authorize the use of SSUET information systems and its conditions. Those who are authorized must be:

(1) current faculty members, staff, and students of the University
(2) others whose use is consistent with the University's mission and whose usage does not interfere with others' access to resources.

For resources and services managed at the unit level, the Director IT may delegate responsibility to the managing unit, both for defining appropriate use and designating authorized users. In all cases, though, both the authorization and the conditions of use must be consistent with the education, research, and service mission of the University, and be consistent with this policy.

5 Responsibilities and Privileges

Each campus community member is accountable for his or her actions as a condition of continued membership in the community. The interplay of privileges and responsibilities engenders the trust and intellectual freedom that form the heart of our community. To maintain this trust and freedom, each person must develop the skills necessary to be an active and contributing member of the community.

Authorized users must fulfill certain obligations as part of and in their use of SSUET information systems. Similarly, there are fundamental privileges common in the academic community, several with counterparts in the cyber world. These responsibilities and privileges are found in the following non-exhausted list, but it

must be understood that no privilege is absolute nor without limitation. Additional detail and clarity, where appropriate, appear in subsections after the list.

a) Authorized users of SSUET information systems must be mindful of the impact their use may have on others with a legitimate interest in using SSUET information systems.
b) Authorized users of SSUET information systems must protect the authentication credentials they use when accessing SSUET information systems.
c) Authorized users of SSUET information systems must be responsible stewards of the resources to which they have access.
d) Authorized users of SSUET information systems are responsible for the proper maintenance, security, and compatibility of their devices connected to the SSUET network or used to access SSUET information systems.
e) Authorized users of SSUET information systems must report any cybersecurity event through the appropriate SSUET channels and cooperate in any investigations.
f) Principles of academic freedom extend to the use of SSUET information systems by authorized users.
g) Principles of expectation of privacy extend to the use of SSUET information systems by authorized users.
h) Principles of ownership for intellectual work products extend to the use of SSUET information systems by authorized users.
i) Individuals must abide by reasonable administrative directives issued by SSUET from time to time concerning the access or use of SSUET information systems.

5.1 Responsible Use of Resources

The use of SSUET information systems must be consistent with the University's mission and values and comply with the normal standards of civil, ethical, and legal behaviour. SSUET information systems are assets shared by the SSUET community. As such, individuals should be mindful of the impact their activities may have on others and their use of information resources. Individuals must be respectful of the finite capacity of the resources and refrain from consuming excessive amounts of network bandwidth or other system utilities. Incidental personal use, including recreational, is permitted provided it does not impede the legitimate activities of others and is not otherwise prohibited by the unit in control of the resource.

5.2 Protection of Access Credentials

The use of SSUET information systems granted to an authorized user is for that person's sole use. Generally, access credentials (e.g., user identifier and password) are needed to identify the authorized user and enable access to the resource. Authorized users are responsible for the security of their access credentials. Access credentials must not be shared with others under any circumstances whatsoever.

5.3 Information Stewardship

Authorized users of SSUET information systems may, as part of their authorized use, have access to information resources belonging to SSUET or others. The use of the information must be limited to what is authorized. In addition, the authorized user must not handle the information in a way that puts it at risk of alteration or deletion or exposure to others not authorized to access the information.

Moreover, even when confidential information is exposed inadvertently, individuals should respect the confidentiality the information warrants.

5.4 Antivirus/Spyware Software

Devices connected to the SSUET network or used to access SSUET information systems should be compatible with the purpose and capabilities of the SSUET information systems and should have their software components well-maintained. Devices with unsupported operating systems or application software, or lacking applicable security patches, are vulnerable to cyberattacks. They put themselves at risk of a data breach or worse; they also put the rest of SSUET's network at risk of a data breach or worse.

Individuals are responsible for devices they use to access SSUET information systems, and for devices they connect to SSUET's network. Devices that are not compatible with the SSUET information systems' capabilities or its purpose or that are improperly maintained or that show signs of compromise from a cyberattack may be isolated from the rest of the SSUET network or removed from the network entirely and denied access to SSUET information systems.

5.5 Security Incident Response

Cyberspace is an astoundingly rich resource of information, products, and services. It is also astoundingly hostile to unsuspecting people and equipment. Attacks attempting to exploit vulnerable computer systems or to lure individuals into scams or frauds are continual. No amount of due-diligence can protect everything that needs to be protected all the time. Now and then, an attempt will succeed.

Individuals are obligated to report all suspected security incidents immediately without any delay. An investigation may be required to assess the impact of the suspected incident; individuals are required to assist with any such investigation.

Through his or her Information Security Office, the Director IT is responsible for promulgating procedures for responding to security incidents.

5.6 Freedom of Expression

In keeping with its long tradition of academic freedom, SSUET supports free inquiry and expression in the use of SSUET information systems. SSUET, however, reserves the right to take action against or deny access to its facilities to those whose use is not consonant with the purposes of the University or infringes on others' rights.

5.7 Privacy

SSUET acknowledges that privacy is an important value for educational institutions. Creative, innovative, and risky thought and scholarship and academic accomplishment depend on interacting in a communication context in which individuals feel free to express and transmit their opinions and ideas.

Thus, SSUET extends to its authorized users a reasonable expectation of privacy in their activities using SSUET information systems. However, everyone should recognize that privacy cannot be guaranteed, even when it is intended. While SSUET does not monitor individual authorized users' online activities, personal privacy may be compromised in an unintentional, incidental way during routine information system operation or maintenance, and it may be infringed in a more deliberate way when so authorized with a cause.

SSUET may access or disclose activity log records for an individual or group using SSUET information systems or the information files or communications stored on or transmitted by SSUET information systems

(1) when there is reason to believe SSUET policy has been violated
(2) to preserve SSUET rights and assets
(3) when compelled by legal process. The determination is made by the Vice-Chancellor with the concurrence of the Registrar and/or the Director IT.

5.8 Ownership of Intellectual Works

Individuals creating intellectual works using SSUET information systems, including but not limited to software, should consult The SSUET Intellectual Property Policy.

5.9 Social Media

Interactive computer-mediated technologies that facilitate the creation and sharing of information, ideas, and other forms of expression via virtual communities and networks.

Social media platforms include Facebook, Twitter, Instagram, LinkedIn, Reddit, and many others.

5.9.1 Guidelines

SSUET's social media guidelines are set forth to serve as a touchstone to help all SSUET community members who use social media to promote the University's work and culture. These guidelines are intended to be considered together with and do not replace existing policies or procedures.

For those members of the SSUET community who manage or maintain social media accounts specifically to represent SSUET entities (such as academic or administrative units, labs, or clubs), there are additional expectations of you and additional resources available to you.

5.9.2 For everyone in the SSUET community

5.9.2.1 Be respectful

Positive and negative content are legitimate parts of any conversation. It's okay to accept the good and bad, but not the ugly. Know your audience and consider how your post could affect them -- before you post. And don't tell other people's personal information or information you have obtained in confidence or violate their intellectual property rights. Make sure you understand SSUET's policies on electronic resources, harassment, etc.

Always keep in mind SSUET's Honor Code, which states that "no member of the SSUET community shall take unfair advantage of any other member of any community."

5.9.2.2 Be authentic

Represent yourself accurately and be transparent about your role at SSUET if it pertains. Admit when you make mistakes and correct inaccurate information. Consider that you are in an academic environment.

5.9.2.3 Be engaged

Social media provides a place to foster community and conversation – be part of that!

5.9.2.4 Be aware

Social media is "real life." How you behave and communicate should be no different than you would via email, public speech, classroom lecture, conversation with friends, or a poster on a wall. Anything considered inappropriate offline is likely also inappropriate online. When in doubt about whether to share or not, it's better to be safe than sorry. Publishing on a social network is still publishing – if you don't want something shared rapidly with the world, better not to post online.

5.9.3 For those representing SSUET entities

5.9.3.1 Be on-brand

Remember that you are representing your organization as well as the University. Members of the SSUET community must not represent their personal opinions as approved or endorsed by the University. The SSUET name and representative symbols must not be used to endorse or support any idea, product, private business, cause, or political candidate.

Ensure that anyone following your account knows who you represent. We discourage individuals from using personal

accounts as representatives for a division or unit, knowing that people's roles with the University may change or cease.

If you are posting from a personal account and identify yourself as being associated with SSUET, please include a disclaimer in your bio/profile that clearly states "*the opinions represented here are my own, not those of SSUET*."

Please ensure that you are following the most up-to-date editorial style guidelines and Brand Identity Guide.

5.9.3.2 Be prepared

Plan your strategy before launching a new account or campaign – reach out to the Marketing Department and the Registrar's Office for help if you need it. Prepare your comment policy and community guidelines before you need them. Ensure at least two SSUET employees have up-to-date access credentials for any account.

5.9.3.3 Be accurate

If you can't validate it, don't post it.

5.9.3.4 Be responsive

If you maintain an account representing the institution, you are a customer service representative for the brand. Reply to questions, even if the answer is basic, such as "*we encourage you to review the information available on ssuet.edu.pk*" or "*we encourage you to reach out to SSUET for the answer to your question*." You are also expected to moderate comments actively (when/where applicable) that may be in violation of the host site's terms or which may be seen as or are otherwise inappropriate in any manner whatsoever.

5.9.3.5 Be good

Ensure you are aware of and adhering to the terms and conditions set forth by any social network you choose to employ. Be responsible for understanding the basics of copyright law and ensuring you behave legally and ethically regarding other people's work. Obtain permission before posting a photo of someone.

5.9.3.6 Be safe

Ensure you are following best practices for safe computing and routinely checking your accounts for any evidence of intrusion.

5.9.3.7 Be data-driven

Don't "spray and pray." Social networks provide valuable data related to the things you share. Make a plan and regularly review your successes and failures to advance your efforts.

5.9.3.8 Ask for help

If you are unsure about a post's appropriateness or find yourself on the receiving end of abuse, threats, or other red-flag behaviour, bring your concerns to the Registrar's Office and the Marketing Department immediately.

5.9.3.9 Groups, Pages, Blogs, and other Social Media

All Blogs, Websites, Pages, and Groups associated with or about SSUET and being managed by SSUET personnel on any digital platform must be listed with/and approved by the University. Until such time as the existing page/site has been approved, the site MUST be suspended.

All content on these sites/pages must conform to all sections in this policy, and the Student, Faculty and Staff Handbooks.

A university nominated moderator with admin rights MUST be given access to the page/site

5.9.3.10 Be Honest and Loyal

You are prohibited from sharing any information/post/media that is misrepresenting/misleading or content that defames the University in any way or form.

6 Prohibitions

Prohibited activities involving SSUET information systems are found in the following non-exhaustive list. Additional detail and clarity, where appropriate, appear in subsections after the list.

a) Individuals must not share passwords or other access information or devices or otherwise authorize any third party to access or use SSUET information systems on their behalf.
b) Individuals must not engage in unlawful or illegal activity nor activity in violation of SSUET policy.
c) Individuals must not engage in any unauthorized access or unauthorized use of SSUET information systems.
d) Individuals must not use SSUET information systems to breach or violate confidentiality obligations or privacy requirements, including collecting or harvesting confidential information.
e) Individuals must not use SSUET information systems to misappropriate or violate the rights of any third party, including using SSUET information systems to store, receive, send, or make available materials protected by intellectual

property rights of third parties without the permission of the owner of the intellectual property rights, unless otherwise permitted by applicable law.

f) Individuals must not damage, disrupt, tamper or interfere with, diminish, or render inaccessible or unusable SSUET information systems, SSUET's or others' equipment, software, data, communications, or use of SSUET information systems, or attempt to do so, or encourage or assist others to do so.
g) Individuals must not initiate a denial of service attack from or against SSUET information systems or release a virus, Trojan horse, worm, or other malware or spyware from or against SSUET information systems.
h) Individuals must not use SSUET information systems to engage in fraudulent activity nor to perpetrate a hoax or engage in phishing schemes or forgery or other similar falsification or manipulation of data.
i) Individuals must not use SSUET information systems to abuse, harass, stalk, threaten, cyberbully, unlawfully discriminate against, or otherwise violate the rights of others nor to libel or defame others.
j) Individuals must not resell or charge others for SSUET information systems, either directly or indirectly, except as authorized by SSUET.
k) Individuals must not take any action that encourages or assists others in engaging in any acts prohibited under this policy (including providing others with the ability to access data or resources they should not be able to access).
l) Individuals must not use SSUET information systems to misrepresent their identity or impersonate any person.
m) Individuals must not use SSUET information systems to participate in pyramid schemes or chain letters.
n) Individuals must not use SSUET information systems for commercial purposes that are unrelated to SSUET in an official way.

6.1 Conduct and Misbehavior

The tenets of cyber citizenship are founded in the tenets of ordinary citizenship. Standards of behaviour for the SSUET community apply both to real-world actions and to those committed in a cyber context.

No individual may use SSUET information systems to violate SSUET policy or the law. Cyberbullying is still bullying. Online snooping is still an invasion of privacy. Neither the unique abilities nor the sense of anonymity possible online empowers individuals to misbehave.

6.2 Unauthorized Access

All use of SSUET information systems must be authorized. Except for those cases where the information systems are intended for general public use (e.g., SSUET’s web presence), the authorization must be explicit.

No individual may use SSUET information systems without authorization, nor may SSUET information systems to be used to access the information systems of others in unauthorized ways. This prohibition is not limited to just the information system itself; it extends to the information stored on, processed by, or transmitted to or from the information system as well.

The absence of effective access control may not be interpreted as authorization to access a system or resource. Individuals must not attempt to circumvent any access control, and they must not examine, alter, copy, nor delete information resources without a reasonable expectation that permission to access the resource was intended.

6.2.1 Privileged Access

Staff personnel with responsibilities for the maintenance, operation, and administration of SSUET information systems may be granted special privileges needed to perform their job responsibilities.

Individuals with special privileges may use them only to the extent necessary to perform the duties of their position reasonably.

No one may exploit a special privilege or ability to monitor the activities of any individual or group in their use of SSUET information resources, to intercept information in transit, nor to examine, alter, copy, or delete information resources belonging to other authorized users except where explicitly authorized according to this policy.

6.3 Intellectual Property

Intellectual property is a fundamental asset for any university. SSUET requires its property rights in research results, inventions, course design, and all other results of scholarly pursuit be respected and not be infringed in any manner whatsoever. To complement this requirement, SSUET requires that the intellectual property rights of others be respected as well.

Intellectual property rights most commonly fall under copyright, patent, trademark, or non-disclosure agreement, but regardless of the protection, SSUET information systems must not be used to infringe on the intellectual property rights of others.

6.3.1 Copyright

Copyright applies to certain forms of creative works such as literary and artistic production. Included under copyright protection are books, maps, reports, and other publications, and also such things as sound recordings, films, photographs, software, and architectural works. Copyright includes the right to reproduce, distribute, publish (which is interpreted broadly to include perform or display), and create derivative works of the original. The rights granted to the copyright holder are exclusive, but they are not absolute. The rights are exclusive in the sense that others are prohibited from using the work without the holder's permission, but they are not absolute because there are limitations and exceptions, most notably under the principle of Fair Use.

The use of material protected by copyright requires either the copyright holder's permission or an exemption under Fair Use.

6.3.2 Software

Software falls under copyright, but distribution is typically not by the sale of copies of the work. Instead, the software is licensed for use under a set of terms and conditions. Software products must not be installed or used on SSUET information systems unless they are properly licensed for the purpose.

Special caution is required for products available in "personal use" or "trial" versions. Personal- use editions are often restricted to non-commercial use by an individual on personally-owned equipment at home. The software of this sort must not be used on SSUET information systems.

Trial versions may forbid any sort of production use. The trial version is intended for evaluating the software product for some purpose, not for conducting the business of the organization. Trial-version software must not be used on SSUET information systems for other than the permitted purpose.

6.3.3 Entertainment

The intellectual property of the entertainment industry (e.g., music, television, motion picture) falls under copyright. However, the ease with which digital copies of material can be made and then distributed without regard to the copyright holder's intention has made intellectual property "piracy" an especially acute problem for the entertainment industry.

The entertainment industry has been aggressive in defending its rights. On occasion, this has led to lawsuits seeking substantial sums of money in damages for copyright infringement. Individuals should be aware that the legal consequences for piracy rest on the individual, not the University. SSUET shall not be responsible or liable, whether directly or indirectly, for legal action or in damages or in any other way whatsoever for such breaches/piracy

6.4 Personal Use

Personal use of SSUET information systems falls outside of their general purpose. Personal use is generally not allowed except:

(1) where the activity is incidental in nature, both in terms of resource consumption and the financial value of the activity
(2) does not impede the legitimate activities of others using SSUET information systems
(3) does not interfere with employee work responsibilities
(4) is consistent with community standards and all other SSUET policies.

Personal use for the benefit of any commercial third party is prohibited, as is facilitating access for a third party to SSUET information systems for which the third party would not otherwise have authorized access.

Special exemptions may be granted for activities deemed aligned with SSUET's interests. Director IT has the authority to grant exemptions.

6.5 Misrepresentation

No one may use electronic communication, including its various forms as social media, in an attempt to impersonate another person or otherwise misrepresent oneself to others. Although there are instances in which anonymous communication (or communication under a fictitious identity with no intent to deceive) is acceptable, it is generally advisable to identify oneself accurately.

7 Personal Devices

While SSUET grants its Students, Faculty and Staff permission to use their smartphones, tablets, and laptops at the University for their convenience, SSUET reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of SSUET's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Specifically related to device security and measures against hacking/malware/spyware etc.

7.1 Acceptable Use

- The University defines acceptable business use as activities that directly or indirectly support the business of SSUET.
- The University defines acceptable personal use on university time as reasonable and limited personal communication or recreation, such as reading or playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the University's discretion. Such websites include, but are not limited to…
- The devices' camera, video capabilities and sound recording are not disabled while on-site.
- Devices may not be used at any time to:
  - Store or transmit illicit access materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
  - Etc.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)

- The following apps are not allowed: (apps not downloaded through iTunes or Google Play, VPN networks, etc.)
- Employees may use their mobile device to access the following university-owned resources: email, calendars, contacts, documents, etc.
- SSUET has a zero-tolerance policy for texting or emailing while driving, and only hands-free talking while driving is permitted.

7.1.1 Devices and Support

- Smartphones, including iPhone, Android, Blackberry, and Windows phones, are allowed.
- Tablets including iPad and Android are allowed (the list should be as detailed as necessary, including models, operating systems, versions, etc.).
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for the operating system or hardware-related problems.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software, and security tools before they can access the network.

7.1.2 Reimbursement

- The University will/will not reimburse the employee for a percentage of the cost of the device (include the amount of the University's contribution), or The University will contribute X amount of money toward the cost of the device.
- The University will a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan, etc.
- The University will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

7.1.3 Security

- To prevent unauthorized access, devices must be password protected using the device's features, and a strong password is required to access the university network.
- The University's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers, and symbols. Passwords will be rotated every 180 days, and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.

- After five failed login attempts, the device will lock. Contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees are automatically prevented from downloading, installing, and using any app that does not appear on the University's approved apps list.
- Smartphones and tablets that are not on the University's list of supported devices are/are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.
- Employees' access to university data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus, or similar threat to the security of the University's data, and technology infrastructure.

7.1.4 Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the user's personal data from being lost in the event it must remote wipe a device; it is the user's responsibility to take additional precautions, such as backing up their data.
- The University reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the University within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices ethically at all times and adhere to the University's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of University and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- SSUET reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

8 Relationship to Other Policies

The IT and social media policies and procedures are a University-wide policy. It supersedes all previous policies on the same subject. This policy has a peer relationship with other University-wide policies where it is primary for the specifics of activities involving SSUET's network and its information resources and services; others are primarily for their respective areas.

a) SSUET Policies – These policy documents define elements of acceptable and unacceptable behaviours by the faculty, staff, and student body. Those elements must be consonant with this Cyber Citizenship Policy. These documents also specify how violations of policy, including this policy, are adjudicated.
b) Intellectual Property Policy – This policy defines the terms and conditions for ownership and protection of intellectual property created by members of the SSUET community.
c) Conditions of Use statements – Components of the SSUET information system may have explicit statements delineating how the individual systems may be used, usually in line with the systems' intended purpose. The statements may be more restrictive than the Cyber Citizenship Policy, but they still must be consistent with it.

9 Reporting Violations

Questions that may arise about this policy or whether something would violate its tenets may be directed to the office of the Registrar or Director IT.

Except as provided otherwise in this policy, suspected incidents that would violate other University-wide policies should be reported in accordance with the other policy. Some violations of this Cyber Citizenship Policy will have no clear parallel in other policies (or the parallel may be unknown), in which case suspected violations might be reported to the Registrar's office.

10 Enforcement and Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including, but not limited to, the loss of access to SSUET’s network and its information resources and services, disciplinary action, dismissal from the University, and legal sanctions under the law of Pakistan.

Incidents involving students, faculty members, or staff members will be handled according to procedures found in the respective handbooks for students, faculty, staff,and guidelines established by the Board of Governors, the Vice-Chancellor, or the Registrar, as appropriate.

Some violations may constitute criminal offences. These may be referred to law enforcement authorities for prosecution.