



JMJ



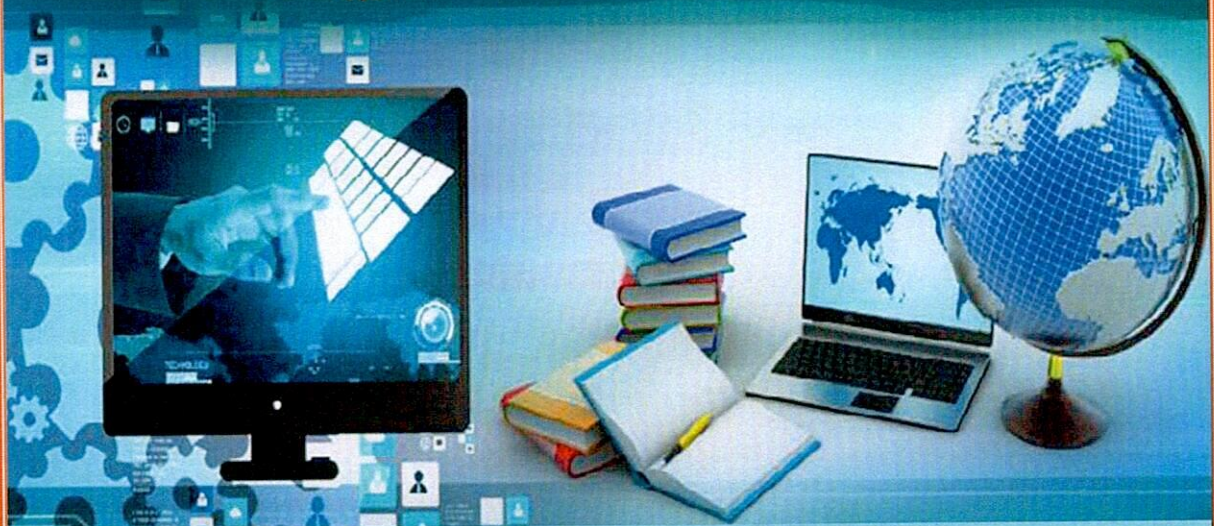
ISO Certificate No.
Q9186414992

COLLEGE FOR WOMEN (AUTONOMOUS), TENALI - 522 202

Affiliated to Acharya Nagarjuna University



Rev. Fr. MATHIAS WOLFF S.J.
FOUNDER - SOCIETY OF JMJ



IT POLICY

BACKGROUND AND SCOPE:

JMJ IT Policy is intended to describe best practices to ensure availability, integrity, reliability, privacy and confidentiality of the college computers, information systems, data and networks. JMJ College makes computing and network resources available to faculty, staff and students and to some extent the general public, to support the educational, scholarship, research and service mission of the college.

The policy supplements other JMJ College policies and procedures, including, the e-mail policy, File sharing policy, social media policy, and connecting devices to the JMJ College network policy, should be read together with those policies.

The college reserves the right to amend this policy at its discretion with or without notice. In case of amendments to the policy, JMJ College will make efforts to inform users of changes.

POLICY AND USER RESPONSIBILITIES:

JMJ College's computing and network resources should be used wisely and carefully with consideration for the needs of others. By using the college computers, information systems, and networks, user of college computing resources, assume personal responsibility for acceptable use in conformity with this policy, other applicable JMJ College policies, and with applicable federal, state and local laws and regulations.

All communications and information transmitted by or through, received by or from, or stored in these systems are JMJ College records and property of JMJ College. No right of personal privacy in any matter stored in, created, received or sent over JMJ College computers, storage devices, email, internet, or voicemail system.

Be aware that even deleted or erased computer, e-mail and voicemail messages may remain stored in JMJ College computer servers or telephone systems. By placing information on JMJ College's computer systems or servers, or using any JMJ College equipment, you have consented to JMJ College's right to capture, edit, delete, copy, republish and distribute such information.

JMJ College provides access to Internet services such as web browsing. Use of the college internet services are only for educational use. This restriction includes any internet service which is accessed on or from JMJ College premises using JMJ College computer



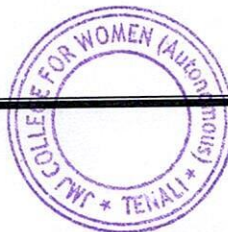
equipment or via JMJ College paid access methods and/or used in a manner that identifies you with JMJ College.

The following is a non-exclusive list of prohibited use of JMJ College technology resources. JMJ College reserves the right to prohibit any use of its computing facilities by any person(s) if and when such use appears to be inconsistent with this policy, other computer use policies, the mission of the college, or any applicable federal, state or local law.

Prohibited Uses:

All users may not...

1. Attempt to use technology resources without proper authorization;
2. Attempt to obtain privileges or access for which you are not authorized;
3. Attempt to learn another user's password(s) or personal information;
4. Attempt to alter or obscure your identity or your computer's identity, including IP Address and email address, while communicating on any network, system or application;
5. Attempt to access, modify and/or delete another user's files, configuration or application without the expressed agreement of the owner or by an JMJ College administrator;
6. Share confidential computer, system, application, or network password with any other person;
7. Attempt to interfere with or disrupt computer or network accounts, services or equipments, IT resources (like LAN or Internet bandwidth) through the propagation of worms, Trojans or viruses;
8. Attempt to "crash" any college computing facilities, including any so called "denial of service attack";
9. Attempt to monitor, intercept, analyze or modify network traffic or transactions;
10. Attempt to alter or reconfigure any JMJ College IT resources, (ex: network infrastructure, servers, wireless);
11. Attempt to use unauthorized devices when connecting to the JMJ College network- view device policy on the JMJ College website.
12. Attempt to remove, duplicate or export confidential/ sensitive JMJ College data in any digital format, outside of JMJ College systems and network, without prior written consent



by JMJ College administrator. This includes any/all data stored: on-premise and/or externally hosted third party provider.

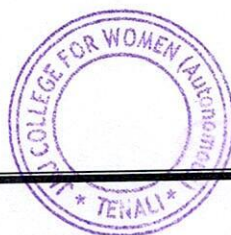
- Examples of confidential/ sensitive information include, social security numbers; financial account information; Family Education Rights and Privacy Act (FERPA) protected records, Health Insurance Portability and Accountability Act protected records; employee records; and accounting records.
13. Attempt to use computing or network resources for profit or commercial gain outside of official JMJ College.
 14. Download and/or share copyrighted material for which you do not have proper authorization.
 15. Attempt to copy software or any intellectual property in a manner that appears to violate copyright law, or otherwise infringing on any intellectual property rights of others;
 16. Compose, transmit, or access data containing content that could be considered discriminatory, offensive, pornographic, obscene, threatening, harassing, intimidating, or disruptive to any other person. Examples of unacceptable content may include, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, color, religion, creed, sex, gender, gender identification, sexual orientation, ethnicity, national origin, ancestry, age, disability (including HIV-AIDS status), marital status, military status, citizenship status, predisposing genetic characteristics or any other characteristics protected by law.
 17. Consume any food or drink in any JMJ College computer lab.

FEDERAL, STATE AND LOCAL LAWS:

All computer and network users are bound by applicable federal, state and local laws relating to harassment, copyright, security, and privacy relating to digital media.

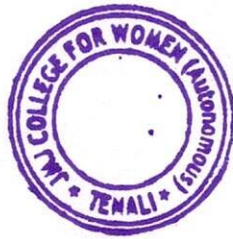
POLICY ENFORCEMENT:

JMJ College at all times retains the right, without notice, to search all directories, indices, data storage devices of any type, files, databases, e-mail messages, voice mail messages, internet access logs and any other electronic transmissions contained in or used in



conjunction with JMJ College computer, e-mail, voicemail and internet access systems and equipment.

Administrators will investigate alleged violations of this policy in order to ensure compliance. Computer department may restrict individuals from the use of computers and networks where violations of this policy of federal, state or local laws is suspected or found. Violations of this policy by a student may result in disciplinary action.




Principal
PRINCIPAL
JMJ COLLEGE FOR WOMEN (Autonomous)
TENALI