MADRAS SCHOOL OF SOCIAL WORK
32, CASA MAJOR ROAD, EGMORE, CHENNAI - 600008

Information Technology (IT)

Policies, Procedures & Guidelines

Prepared by

UGC-Network Resource Centre
Madras School of Social Work
2021

TABLE OF CONTENTS

1. About the UGC-Network Resource Centre

Since 1987, the University Grants Commission has been assisting colleges in procuring basic Information & Technology infrastructure like personal computers and other peripherals. Through the X and XI Plans, the UGC assisted MSSW to establish the "UGC – Network Resource Centre (UGC-NRC)" and provided grants for the purchase of computers and internet connectivity. Since then, MSSW has been providing computer and internet facilities to students and faculty members. The computer lab is equipped with 20 desktop computers with 100mbps internet connectivity. Students are also provided with WiFi connectivity inside the campus. Thus, the centre strives to create a digital learning environment for the students at MSSW.

2. Vision & Mission

Vision

- The power of IT is leveraged to the fullest possible extent to facilitate teaching, learning, research and digital campus management.

Mission

- To provide uninterrupted digital connectivity to the entire campus
- To ensure quick access of data and information to all users
- To deploy a digital campus management system that provides seamless information management across processes.
- To implement an advanced Learning Management system for digital learning opportunities.

3. History

- The Internet Center was established in the year 2004 with 10 computers with 256Kbps speed internet connectivity catering to the internet browsing requirements of students and research scholars.
- In 2015, the campus was equipped with a PA system facility in each class room and Open Air Auditorium. This facility was widely used for college assembly programs and for the principal's addresses on important occasions.
- During 2016-2017, high speed optical fiber network connectivity was installed, providing 100 MBPS high speed internet to all the parts of the MSSW campus.

- During 2017, Wi-Fi facility was also extended to the whole campus.
- In the year 2018, internet connectivity in MSSW was enhanced to 1GBPS .
- Since 2018, all classrooms have been enabled with smart class room facilities.
- An MOU has been signed with Jio for creating Wi-Fi access inside our campus with 32mb of data per user login.

Functions

The centre for Computing provides the following facilities to the users.

- Campus internet connectivity
- Wi-Fi networking
- Computer (Desktop & Laptop) maintenance for faculty and office staff
- Student internet browsing facility
- Video conferencing facility (AV Hall, MCJ Building)

Internet Centre

- The centre is equipped with 21 computers with internet connectivity.
- Faculty members, students, and research scholars are permitted to use the facility.
- It is used for providing training to students, for online tests & interviews.
- Campus Optical Fiber BSNL, and Atria Convergence Technologies (ACT) distribute high speed internet connectivity to all buildings on the campus through a high speed Gigabyte (100/1000Mbps) LAN Switch.

Internet centre services

- New connections
- Maintenance
- Modifications / relocations
- Wi-Fi Access Points (AP) installations
- Use of secured and authenticated internet networks

Wireless Network (Campus Wi-Fi)

- 18 AP's through D-Link & TP Link controller with management & control features.
- Capable of connecting PCs, Smart phones & Laptops through secured wireless encryption using WPA OR WPA2, Wi-Fi protected Setup (WPS)
- Outdoor internet café is available at four central locations.

- Wi-Fi is offered in classrooms and hostel buildings.

Video Conferencing Facility (AV Hall)

- Established during 2017-2018
- Installed at AV Hall, MCJ Building (1st Floor) and also available at Auditorium and Conference Hall
- Used for remote class rooms, online classes/live sessions, webinars, online interviews, online PhD viva voce examinations

4. Need for IT policy

- An Information Technology (IT) Policy identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources.
- IT policies and procedures provide clarity for everyone in an organization regarding information technology.
- IT policies work to combat threats and manage risk while also ensuring efficient, effective, and consistent operations.
- Information security functions based on three things:
    - ◊ **Confidentiality** - information must not be made available or disclosed to unauthorised individuals, entities, or processes.
    - ◊ **Integrity** - data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes.
    - ◊ **Availability** - information must be accessible and usable on demand by authorised entities
- In recent days, especially due to COVID-19, online teaching and learning has gained momentum in the college. All the departments are using the online mode of communication, right from admitting students to generating transfer certificates. Undoubtedly, Intranet & Internet services have become the most important resources at Madras School of Social Work.
- Therefore, Madras School of Social Work has decided to have its own IT Policy that works as guidelines for using the college's computing facilities including computer hardware, software, email, information resources, intranet and internet access facilities, collectively called "Information Technology (IT)".

- Due to the dynamic nature of Information Technology, information security in general and therefore policies that govern information security processes are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

- The purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help the college, departments and individuals who are part of MSSW to understand how MSSW's IT policy applies to some of the significant areas of work and to bring them into conformance with stated policies.

5. Applicability of the policy:

This policy applies to all **students, faculty, and staff of the College and to all other users of information technology resources** at Madras School of Social Work. These users are responsible for reading, understanding, and complying with this policy.

Certain violations of IT policy laid down by MSSW by any user may even result in disciplinary action against the offender by the college authorities. If the matter involves illegal action, law enforcement agencies may also be involved.

6. E-Mail Account Use Policy

Formal communication like circulars, documents, important announcements will be sent to staff and students through the official E-mail IDs. In order to receive such communications all the staff and students are provided with an official E-mail ID.

E-Mail ID for Staff

- To avail of an official E-mail ID, the staff shall submit their E-mail ID request to the administrative officer (ao@mssw.in) mentioning their first name, last name, personal E-mail ID and mobile number.
- E-Mail IDs will be created and the login credentials will be mailed to their personal E-mail ID provided in the request letter/email. It will take one working day to receive the E-mail login credentials. The password can be changed by the user while signing in for the first time.

- Contact the coordinator of UGC-Network Resource Centre (admin@mssw.in) to re-set the password or for any other technical issues related to the official E-mail ID.

E-Mail ID for Students

- To avail of an official E-mail ID, the students shall follow the guidelines and submit it to the department head. (Download Template)
- E-Mail IDs will be created and the login credentials will be mailed to the respective department head. It will take two working days to receive the E-mail login credentials for students. The password can be changed by the user while signing in for the first time.

7. Website Policy

Terms and Conditions

The website is designed, developed and hosted by MSSW. Though all efforts have been made to ensure the accuracy and currency of the content on the college website, the same should not be construed as a statement of law or used for any legal purposes. MSSW accepts no responsibility in relation to the accuracy, completeness, usefulness or otherwise, of the contents. Users are advised to verify/check any information with the relevant department(s) and/or other source(s), and to obtain any appropriate professional advice before acting on the information provided on the website.

In no event will MSSW be liable for any expense, loss or damage, including, without limitation, indirect or consequential loss or damage, or any expense, loss or damage whatsoever arising from use, or loss of use, of data, arising out of or in connection with the use of this website.

Links to other websites that have been included on this website are provided for public convenience only. MSSW is not responsible for the contents or reliability of linked websites and does not necessarily endorse the views expressed in them. We cannot guarantee the availability of such linked pages at all times.

Copyright Policy

Material featured on this website may be reproduced free of charge after taking proper permission by sending an email to us. However, the material has to be reproduced accurately and is not to be used for any derogatory purpose or in a misleading context. Wherever the material is being published or issued to others, the source must be prominently acknowledged. However, the permission to reproduce this material shall not extend to any material which is identified as being copyright of a third party. Authorisation to reproduce such material must be obtained from the departments/copyright holders concerned.

Privacy Policy

Our website or apps do not automatically capture any specific personal information from you, (like name, phone number or e-mail address), that allows us to identify you individually.

If MSSW requests you to provide personal information, you will be informed about the particular purposes for which the information is gathered and adequate security measures will be taken to protect your personal information.

We do not sell or share any personally identifiable information to any third party (public/private). Any information provided on the website will be protected from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

We gather certain information about users, such as Internet protocol (IP) addresses, domain name, browser type, operating system, the date and time of the visit and the pages visited. We make no attempt to link these addresses with the identity of individuals visiting our site unless an attempt to damage the site has been detected.

Hyper Linking Policy

Links to external websites/portals

At many places on this website, you shall find links to other websites/portals. These links have been placed there for your convenience. MSSW is not responsible for the contents and reliability of the linked websites and does not necessarily endorse the views expressed in them. Mere presence of the link or its listing on this website should not be assumed as endorsement of any kind. We cannot guarantee that these links will work all the time and we have no control over the availability of linked pages.

Links to MSSW website by other websites

Prior permission from MSSW is required to link our website on your portals and websites. We would like you to inform us about any links provided to this website so that you can be informed of any changes or updations therein. Also, we do not permit our pages to be loaded into frames on your site. The pages belonging to this website must load into a newly opened browser window of the end user.

8. Hardware & Software IT Policies:

Policy Summary

This policy addresses the installation and configuration of hardware and software in MSSW privileged systems. This policy applies to all equipment (software and hardware) supported by UGC & Society and purchased funds.

Personal Computer: A computer used primarily by one individual. This typically refers to a computer allocated to faculty or staff members. Personal computers generally function as standalone units to which primary access is made via a locally attached keyboard, mouse, monitor, etc.

System Setup and Configuration

The System Administrator is responsible for the setup and configuration of all systems.

Inherently insecure software and system services will be disabled and/or removed from machines. The System Admin is responsible for approving a list of insecure software and services. When it is impossible to find a secure software alternative, the system will be moved to the Computer lab for further action.

System Security

Privileged access requires users to adhere to the following:

- Agree to this IT policy.
- Practice good password management.
- Maintain a password composed of at least eight letters, numbers and special characters or alternating cases.
- Change password regularly.

- Do not transmit passwords in plain text.
- Do not install software or activate system services that are listed on the insecure software and services page

System Admin will consult with the owner of the computer before making any major system changes.

All systems on which faculty and staff have administrative privileges may be periodically scanned for insecure software and services. Failure to follow these guidelines may result in the loss of privileged access and/or the computer being denied access to basic network services (e.g., printing and network).

Software Installation and Licensing Policy:

Basic Software to be installed:

1. Operating system (Win 10,8.1,7)
2. Microsoft Office (Word, Excel, PPT, etc)
3. Adobe Reader
4. WinZip
5. WinRar
6. Wordweb
7. Antivirus (K7)
8. Mozilla Firefox
9. Google Chrome
10. Adobe Flash Player

Any computer purchase made by the System Administrator will have a licensed copy of the following:

1. Operating System:Windows 10 64bit
2. Antivirus: K7 Premium
3. Microsoft Office- Office 2019 (limited access)

9. Network (Intranet & Internet) Use Policy:

Intranet provides local connectivity to the desktops so that IP pooling range should be given separately. Separate LAN Card with Network Interface card with separate MAC address should be implemented for security reasons.

Network connectivity provided by MSSW, through authenticated networks like (BSNL, ACT) access connection is governed by the IT Policy. The Computer lab in charge is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the MSSW network should be reported to the Computer Lab. He will ensure the connectivity by appropriate contact with the service providers.

IP Address Allocation:

Any computer (PC/Laptop) that will be connected to the MSSW network should have an IP address assigned by the admin in-charge. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated an IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorisedly from any other location. As and when a new computer is installed in any location IP has to be allocated according to their Asset Numbers. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately by the Lab in charge.

10. Functions of Computer Lab

- Respond to queries and introduce students to use of computers and peripheral equipment.
- Support faculty and students to use computer software and hardware.
- Extend appropriate procedures, respond to queries and document resolution of repetitive issues.
- Present on software packages and applications and develop lab templates.
- Develop records of students involved in computerized instructional support.
- Manage laboratory software, test materials and hardware to ensure security.

- Watch lab occupants while entering and leaving the lab.
- Ensure proper treatment and authorized removal of equipment.
- Log equipment damage and malfunctions.
- Capture statistical reporting information.
- Offer access to reference manuals and other information to users.
- Extend assistance towards computers and printers' support.
- Clean, review and handle minor equipment maintenance to ensure its operational condition.

11. Video Surveillance Policy

The system comprises Fixed position cameras; Pan Tilt and Zoom cameras; Monitors, Multiplexers; digital recorders; HDD Storage;

Public information signs

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

The system has been installed by MSSW with the primary purpose of reducing the threat of crime generally, protecting MSSW premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:·

Deter those having criminal intent

Assist in the prevention and detection of crimes

Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order

Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students

Assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.·

In the case of security staff to provide management information relating to employee compliance with contracts of employment. The system will not be used for any automated decision taking

On MSSW Campus, we can store 8 days' recording because we are using 16ch and 8ch XVR for recording purpose and motion detection has been enabled for recording purpose to save the HDD space. These CCTV Cameras will be a moral support only. After getting the prior approval from the Principal or from higher authorities' content will be handed over to the concerned person for further action.

12. Guidelines on Computer Naming

Asset Tag Allocation in MSSW:

- Each Desktop and Laptop will be allocated Asset numbering according to their nature of funds. If the fund is allocated by Aided, it will be Tagged with (ADPC) or Desktops and (ADLTP) for Laptops.
- If the fund is allocated by the Society (SSER), it will be tagged with (SFPC) or Desktops and (SFLTP) for Laptops.
- In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network.
- All computer names on the campus network should follow the standard naming convention inside MSSW. Computers not following standard naming conventions may be removed from the network at the discretion of System Admin.

13. Guidelines for Desktop & Laptop Users

The recommendations include the following:

1. All desktop & Laptop users should have the latest version of antivirus and should maintain the setting that schedules regular updates of virus definitions from the Vendor server.
2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. We recommend once in a week cycle for each machine to be updated regularly. Whenever possible, security policies should be set at the higher level and applied to the desktop machines.
3. All Windows desktops should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
4. The password should be difficult to break.

   Password

   i. must be minimum of 6-8 characters in length

   ii. must include punctuation such as ! $ % & * , . ? + - =

   iii. must start and end with letters

   iv. must not include the characters # @ ‘ “ `

   v. must be new, not used before

   vi. Avoid using your own name, or names of your wife or children, or name of your department, or room no. or house no. etc.

   vii. Passwords should be changed periodically and also when suspected that it is known to others.

   viii. Never use ‘NOPASS’ as your password

   ix. Do not leave password blank and

   x. Make it a point to change default passwords given by the software at the time of installation.

5. The password for the user login should follow the same parameters outlined above.
6. The guest account should be disabled.
7. New machines with Windows XP should activate the built-in firewall.

8. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.

11. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

12. In addition to the above suggestions, Computer Admin recommends a regular backup strategy from their usage staff. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

13. If a machine is compromised, System Admin will shut the port off. This will isolate the computer, until it is repaired. At that time, the port will be turned back on.

Don’ts

Files in the below mentioned locations cannot be retrieved when system crashes:

1. Do not save on Desktop.
2. Do not save in Downloads in C: Drive
3. Do not save in Documents in C: Drive
4. Pictures in C: Drive
5. Videos in C: Drive etc.,

14. Guidelines for computer lab users:

Lab timings: 9.30am to 4.30pm

- All students are requested to sanitize their hands and register their names in students're gisters while entering and leaving the lab.
- Wear your ID card and mask when you are in the Lab.
- Systems will automatically shut down at 4.30pm, so users are requested to finish their work on time.
- Remember to shut down the system after usage.
- Maintain silence inside the lab. Avoid chatting and talking in groups. Avoid roaming and unwanted walking in and around the computer lab.
- Mobile phone usage inside the lab is strictly prohibited.
- Leave your footwear outside.
- Avoid using the facility for social networking and entertainment. Anyone found visiting unauthorized sites will be sent out.
- Do not download videos and audio files. Only document download is permitted.
- Only one person can use a system at a time.
- No visitors can accompany the students into the computer lab.
- Use virus-free pen drives.
- Avoid preparing your assignments/reports by sitting inside the lab.
- Eatables/Refreshments are not permitted inside.
- Personal Laptops are not allowed inside the computer lab.
- Please co-operate and make the lab user-friendly.

15. Guidelines for recording and uploading Videos on Youtube

1. Record a session only if it is of value to a larger audience other than the participants.
2. Before recording an online session, obtain the consent of the resource person/panel for the same.
3. Inform all participants of the session that the session is being recorded and may be uploaded on Youtube or any other social media platform.
4. Obtain the consent of the resource person/Panel to upload the session on Youtube.
5. Before uploading edit the content suitably to remove blank screens or any other artefacts that are not appropriate.
6. All such videos of webinars/certificate courses produced at MSSW either independently or in partnership with other organizations must be uploaded only in the official Youtube channel of MSSW. It is convenient for anyone outside MSSW to access all videos at the same place and even for us easy to search and retrieve if it is available at one place. Hence we discourage department wise YouTube channels.
7. As soon as the edited recording is available, you may send the same to Prof. Xavier Vivek Jerry with a brief description for uploading to our official Youtube Channel.
8. There will be a general disclaimer added to the beginning of all webinar videos that “the views expressed in the video are the personal views of the resource person(s) and do not constitute the official opinion/position of MSSW”