

## ICT POLICY

### A. GENERAL GUIDELINES APPLICABLE TO ALL USERS

1. Users shall be responsible for protecting any information used and/or stored online their systems and accounts.
2. Users shall report any weaknesses found in information security, any incidents of misuse or violation of this policy to the proper authorities.
3. Users shall not attempt to access any data or programs on systems maintained by the department for which they do not have authorization or consent of the custodian of the data/programs.
4. Users shall not make copies of copyrighted software except as permitted by law or by the owner of the copyright.
5. Users shall not purposely engage in the activity with the intent to:
  0. Harass other users; degrade the performance of the systems;
  1. Deprive an authorized Department user access to a Department/College resource;
  2. Obtain extra resource beyond those allocated;
  3. Circumvent security measures, or gain access to the system for which authorization has not been given.
6. Electronics & Communication facilities (voice or data) are for authorized use only. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on Office systems.
7. Only authorized users shall download, install or run security programs or utilities that reveal weaknesses in the security of a system (for ex. Vulnerability scanners, password crackers, etc).
8. All users are responsible for adhering to the standards outlined in this security policy document when using college computing facilities.

Any employees/student found to have violated this policy shall be subject to disciplinary action as per the discipline and conduct rules of college.