IT POLICY

1. Title and Applicability

This document is called Information Technology Policy for students. This is binding on all the students using the campus network, computing facilities and communication infrastructure provided by Bharathiar University.

2. Definitions

2.1. **University -** The following Units are parts of Bharathiar University and are jointly and severally included under the term University including but not limited to:

a. Departments

b. Hostels

c. Residential Quarters

d. Controller of Examinations Office

e. Main Office – VC's, Registrar's and Finance Office

f. School of Distance Education

g. Centers

2.2 **Network -** Access and connectivity to the internet provided by the University and/ or systems/devices/ gadgets / servers/ cloud storage /email for the purpose of academics, research, and authorized incidental use.

2.3. **System -** Computing devices/ gadgets/ servers/ cloud storage issued and/provided by University and all computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf.

2.4. **Technology Services –** Data Center of the Bharathiar University.

2.5. **Users -** Any student who is admitted in any department and enrolled for any course under the University until graduation and also includes persons whose physical presence may not be available inside the campus of the University.

3. General Use

3.1. All Users having access to the University's Data, Network and System are responsible for exercising prudent judgment, care and caution and shall be permitted to use the same only to the extent it is authorized and necessary to

fulfill the purpose of academics, research, and incidental use.

3.2. All remote access to networks owned or managed by the University or System must be accomplished using a remote access method approved by the University or System, as applicable.

3.3. All computers and devices used by the Users to connect with the Network whether owned by the User or by the University, should execute virus- scanning software at all times with an updated virus database.

4. Data Center, Bharathiar University:

4.1. University shall have a Data Security Management System to monitor and oversee the Data in the System issued by the University and the Data that is transmitted or processed through the Network issued by the University. Any activity performed by a User using the Data, Network, System or any other information resources of the University, shall be subjected to the Data Security Management System of Bharathiar University.

5. Use of Data, System and Network

5.1. There shall be no usage of Data, System or the Network without proper authorization granted through the University.

5.2. No User under any circumstances is authorized to engage in any activity that is illegal, unlawful or unethical activities under local, state, country or international law while utilizing the Data, System, Network or any other information resources provided by the University.

5.3. If the there is any backup copy of Data of confidential information and intellectual property belonging to the University, on any separate device which is under the personal ownership, the same shall be deleted upon the requirement to access/use such data terminating or upon the instructions of the University.

Further, no user shall use the Data, System or Network:

5.4. To engage in procuring or transmitting material/goods/services that is in is immoral, distasteful, obscene, profane or intended for sexual harassment.

5.5. To cause security breaches or disruptions of Data and Network communication is prohibited. Users must promptly report all information relating to security breaches or disruptions to the Data Center, Bharathiar University at datacenter@buc.edu.in.

5.6. Tampering any computer equipment, whether it belongs to the University or to

an individual is prohibited.

5.7. The unauthorized installation or distribution of pirated software products for use on System or any computer connected to the University's Network is prohibited.

5.8. Violating the rights of any person or any organization protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.

5.9. Providing access to the Network/ System to any third party within or outside of the University to cause the breaches referred herein. In such event, the person providing such access shall be equally responsible for the consequences and penalties thereof.

6. Security control on Electronic Mail (Email) usage

6.1. Communications made through University issued email address should be used for University authorized purpose only.

6.2. Emails sent or received by Users in the course of conducting University activities are Data that are subject to appropriate regulatory records retention and security requirements. The University shall be entitled to access the same in the event of any apprehended breach of clause 5 hereinabove.

6.3. Users must treat all email messages and files as confidential information. Emails must be handled as 'Confidential" and as direct communication between a sender and a recipient. Unless the information owner/originator agrees in advance, or unless the information is clearly public in nature, Users must not forward any email to any email address outside the University's network.

6.4. The following email activities are expressly prohibited when using an University provided email account:

a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account.

b. Accessing the content of another User's email account.

c. Sending or forwarding any email that is suspected by the User to contain computer viruses.

d. Any incidental use violating applicable University policy or accordingto law in force.

e. Any use for the purpose of illegal or unethical activities prohibited bythe University or according to law in force.

7. Password Protection

7.1. University issued passwords or similar information for devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

7.2. System and all electronic devices including personal computers, smart phones or other devices used to access, create or store Data and University information resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.

7.3. Each User shall be held responsible for all activities conducted using the User's password or other credentials. If there is any indication of unauthorized use or change of password, Users shall report the incident to the Data Center, Bharathiar University.

8. Confidential Information, Intellectual Property and Data

8.1. A User is expected to exercise their best efforts of care and caution in protection and proper use of confidential information, intellectual property or Data belonging to the University and to solely utilize the same for the purpose to which a User is authorized to.

8.2. Users must not use or disclose to any confidential information, intellectual property or Data belonging to the University to anyone without appropriate authorization.

8.3. All users have a responsibility to promptly report the illegal, unethical or unauthorized disclosure of University's confidential Information, intellectual property or Data to the Data Center, Bharathiar University.

8.4. Confidential information, intellectual property or Data belonging to the University that is created or stored on a User's personal computers, smart phones or other devices, or in databases that are not part of University's system are subject to all requirements applicable herein.

9. Physical Security of Systems

9.1. Users shall not leave any System unattended. In the unlikely event that the System, including portable computers, smart phones and other computing devices is left unattended, it is the sole responsibility of the User to ensure it is

physically secured.

9.2. Willful destruction of or theft of System or any computing devices belonging to the University is prohibited.

10. Non compliance

10.1. Violations or non-compliance of any one or more of these standards may constitute cause for revocation of access privileges, suspension of access to the System, \ disciplinary action before the Disciplinary Committee of the University and/or appropriate legal action.

11. The University is merely an intermediary and cannot be held liable for any activity performed by the User while using the System, Network or Data. The User assumes absolute and entire responsibility for all his/her action and acknowledges that any breach of the terms herein has been done at his/her entire behest, and the University cannot be held liable for the same. The User acknowledges that the University shall be deemed to be an *"intermediary"* for the purposes of Section 79 of the Information Technology Act 2000, and shall take appropriate action upon any breach/illegality being bought to its attention. The User shall have no claim whatsoever against the University for any action taken in this regard.

12. The University reserves the right to audit all information/ supporting assets/review logs in the event of suspicious activity on the directives of the Technology Services.

13. The University may amend, review and add any policy hereunder as per its discretion. Any usage of the System/Network shall be deemed to be continued acceptance of the terms provided for herein.

14. The terms herein are without prejudice to and in addition to the remedies under law for any illegal/immoral/mischievous act deliberately or negligently caused by the User herein, either directly or indirectly.