CHRIST (DEEMED TO BE UNIVERSITY)

OFFICE OF INFORMATION TECHNOLOGY (OIT)

CODE OF CONDUCT FOR IT END USERS

The Information Technology Resources of the University are intended for effective delivery of the teaching-learning, research, consultancy, innovation and such other related objectives of the University and for its efficient administration. It provides access to wide variety of internal and external information resources. Legitimate use of the Information Technology Resources by the members of the academic community of the University should reflect academic honesty, integrity, diligence and loyalty while using the shared resources and must follow the ethical and legal guidelines as may be applicable. It is the responsibility of every user to respect integrity of the resources, protect the ethical and legal rights of others such as privacy, intellectual property etc. and abide by all applicable and related statutory regulations.

This Code of Conduct made in pursuance of the Regulation for IT shall be applicable to and be binding on all End Users of the Information Technology at the University to ensure legitimacy and propriety of use of the Information Technology Resources.

The Information Technology Resources for the purpose of this Code will mean and include University owned or contracted transmission lines, network, all types of electronic media, servers, ERP System and applications, Internet connections, wireless networks, terminals, personal computers and the devices attached thereto.

The End Users referred to herein will mean and include all the Departments, Centres, Offices, Faculty, Staff and Students of the University in all its Campuses and any other person who has been allotted an Email ID by the University.

The following will constitute the non-exhaustive list of responsibilities of End Users. Prior confirmation of the OIT must be obtained on any question or clarification about the appropriateness of any use of the IT Resources. Authorized users shall be held accountable for violations of this Code of Conduct involving their accounts.

1. **Passwords confidentiality and protection:**
   Passwords are the primary means for the authorised users to access the IT Resources of the University. The Code of Conduct in this regard shall include:
   a) Create and use strong password containing at least eight alphanumeric characters
   b) No User shall share or disclose his/her password(s) to any other person irrespective of their position or standing in the University. Similarly, they must not disclose any other identifying information such as PIN used to access specific system information.
   c) Take care not to save the Login credentials in the browsers while prompted.
   d) Strictly follow the instruction to periodically change the password/s, at least every 90 days. While this will be auto-mandated in the desktop systems of the University, the End User shall ensure this in their personal devices (laptop, mobile etc.)
   e) Log in only when using the System and Log out completely every time after the use.

2. **Use of Information Resources from the Internet:**
   The User may in the course of their authorised activities/role at the University may access or browse through different websites of digital libraries and/or other education related resources whether or not licensed to the University or through other websites of knowledge and information which are available in the public domain. In this regard the Users while using the IT Resources of the University shall ensure:

Registrar
CHRIST (Deemed to be University)
Bengaluru - 560 029

a) In the case of E-Library or E-Books related websites where licensing agreements are signed by the University, to strictly abide by the directions /restrictions applicable thereon as may be advised by the Knowledge Centre of the University.
b) Not to download and put to use any Copyrighted or Patented material, information, logo, brands or artwork by itself or by modifying it, irrespective of whether or not such use may result in any financial gain, without express consent of the IP Rights holder of all such material, information, logo, brands or artwork.
c) Not to browse, upload into or download from any website any unauthorised, objectionable, obscene, and pornographic or such other prohibited material, pictures, films, videos etc.
d) Not to share accounts or network access privileges to anyone to gain access to resources to which they would otherwise be denied.
e) Not to access systems or information not needed in their current role within the University.
f) Not to directly or indirectly compromise the security of any system, internal or external to Information Technology Resources of the University. This includes non-technical activities such as misrepresenting one's identity or impersonating another user
g) Not to illegally access critical data from any networks/websites (internal or external) using Campus Network (Hacking, Sql Injection etc.)
h) Avoid public internet facility to access University applications (Airport Wi-Fi etc.); if required to use ensure to Log out completely after use.

3. Safety and Security of the Equipment and Official Data

It is very important that the User while using the University network either connected to the official desktop within the Campus or to the personal laptop/desktop at home or elsewhere ensure that the computer is fully protected against all perceivable cyber/ digital attacks, both internal and external. In this context the Users shall ensure:

a) To install and maintain genuine non-pirated version of the operating system and the virus detection and eradication software, particularly on personal devices (laptop/tablet mobile etc.) Vulnerability patch updates shall be checked and updated on a regular basis.
b) Not to open phishing, spam and unsolicited email messages and its attachments
c) Not to open any link provided by emails from unknown sources
d) Not to shift /repair or remove Hardware devices in part or full.
e) Not to disturb or alter the Settings of their Computer System.
f) Not to respond to any email seeking personal information without confirming the validity of such mails
g) Not to assign Manual IP for personal devices (laptop/tablet mobile etc.) used.
h) Not to save Application passwords in the browsers while prompted.

4. Usage of Official Email

The User is provided with individual email ID with University network for exclusive use in their official capacity and only for the activities related to the University. The Users are strictly prohibited from using their official email ID for:

a) Any of their personal communication or activities.
b) Unrelated or unauthorised purposes
c) Promoting distrust or discredit about the University or its Faculty or Officers
d) Spamming or such other unethical activities.
e) Sending bulk emails unless, pre-approved by the OIT for authorised purposes.
f) Signing up in Social Media Platforms

5. Harmful and Illegal Activities

No User is permitted to use the Information Technology Resources of the University for any Activity that will cause harm or that is illegal in nature.

The Harmful Activities will mean and include (but are not limited to):

a) Degrading performance or otherwise disabling the Information Technology Resources.
b) Destroying, altering, copying, or compromising information integrity (e.g., student records, personnel information, etc.)
c) Connecting any networking equipment to the campus network or Port scanning or security scanning on the campus network unless pre-approved by the OIT
d) Installing and using any services on their personal laptop or Mobile which will interrupt campus network (DHCP, Broadcasting, Proxy, VPN, Hotspot, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes, torrent, P2P etc.)
e) Email spamming including intentionally introducing malicious codes such as (but not limited to) Viruses, Worms, Trojan Horses, Email Bombs, Spyware, Adware, and Key Loggers.
f) Threatening or intimidating email, postings, or other harmful forms of communication.

The Illegal Activities will mean and include (but are not limited to):

a) Copyright infringement, including publishing copyrighted material such as papers, software, music, musical scores, movies, and artistic works. It is irrelevant whether or not any profit is made from such distribution; the mere fact of providing uncontrolled access to such material is illegal
b) Divulging information that is confidential, private, or proprietary in nature.
c) Misrepresentation of one's identity to gain access to systems, software, or other services to which one does not have authorized access.

Any observed or reported violation of the aforesaid IT Code of Conduct shall also deemed to be violation of the General Code of Conduct specified by the University for Faculty/Staff and Students and the concerned Faculty/Staff or the Student shall be subjected to appropriate disciplinary action as per the relevant Regulations of the University apart from temporary or permanent disabling of the devices used by them from the University Network.

6/12/2021

(Dr Anil Joseph Pinto)
Registrar

Registrar
CHRIST (Deemed to be University)
Bengaluru - 560 029