IT Usage policy and Procedure Manual

of

Guru Gobind Singh Indraprastha University,
Dwarka, Delhi

May 2017

Please upload on Univ. Website

Preamble

ICT Infrastructure is an important element of any higher educational institution. The University provides IT Resources for the advancement of the University's educational (teaching and learning), research, service, and business objectives. It involves huge investment of the University to create such critical assets. It is equally important that the infrastructure so created must be used and maintained to be fully operational and used meaningfully to assist and maximizing the gains from these resources. This Information Technology (IT) policy and procedure manual attempts to provide a guideline document regarding the usage, upkeep, do's and don't's for the Employees (Faculty, Staff) and Students (Research Scholars, Undergraduate and Post-graduate) of Guru Gobind Singh Indraprastha University, Delhi. Any access or use of IT Resources that interferes, interrupts, or conflicts with these purposes is not acceptable and will be considered a violation of this policy.

Purpose:

The main objective of having this policy and procedure manual is:

- To ensure that all employees and students are aware of obligations in relation to use and safety when utilizing information technology within the University Campus.
- To ensure equity among all and enable them to make consistent and reliable decisions.
- give each employee a clear understanding as to what you expect and allow.
- This policy provides notice of the expectations and guidelines of GGSIP University (the University) to all who use and manage Information Technology (IT) resources and services.

Scope:

This policy, and all policies referenced herein, apply to all members of the University community including faculty, students, administrative officials, staff, alumni, authorized guests, delegates, and independent contractors (the "User(s)" or "you") who use, access, or otherwise employ, locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Definitions:

IT Resources include computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, Printers, Scanners, Smart board, Video and Audio conferencing equipment's, data, databases, Internet modems, switches, cables, IP addresses, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

USER RESPONSIBILITIES AND STATEMENT OF PROHIBITED USES

A. Usage

1.Only authorized Users have the privilege to access and use the IT Resources. Access and use is limited to the purposes that are consistent with the instructional, research, and administrative goals of the University.

2. Users are expected to uphold the standards and principles of the University while using the IT Resources and are required to respect the rights of others at all times.

3. Users are prohibited from using any portion of the IT Resources to post or transmit any information, including data, text, files, links, software, chat, collaboration, communication, or other content (Content) that is abusive, disparaging, discriminatory, hostile, combative, threatening, harassing, intimidating, defamatory, pornographic, or obscene.

Users who do not respect the specified Use of IT Resources may be held in violation of this policy.

B. User Names And Login

4. The University makes use of a "user name" or "login", that may be different from the User's legal name for using computing, online or other resources. Using someone else's name or assuming someone else's identity without appropriate authorization, however, is a violation of the University's principles and this policy.

5. Users may not use the IT Resources under false name, identification, email address, signature, or other medium of any person or entity without proper authorization. The University prohibits such use of a User name for the purposes of misrepresentation or an attempt to avoid legal or other obligations.

Any such unethical use may constitute a violation of this policy.

C. Passwords

When choosing a password for access to the IT Resources, or portions thereof, Users must adhere to the following rules so as to prevent unauthorized access through any User's password.

1. Use a different password for each account; and
2. Do not write down your password(s) on a piece of paper or record them in a file.
3. You should change your password every 60 days.
4. Official are expected that the password issued to them are not shared with any other official or student of the university or outside person.

5. Users should avoid using:
   a) Birth dates;
   b) Names (First, Last, or any combination);
   c) Unaltered words that could be found in a dictionary, including non-English words, and words spelled backwards;
   d) Telephone numbers;
   e) Social Security numbers;
   f) Fordham Identification Numbers (FIDN);
   g) Car/Scooter/Mcycle No;
   h) Alphabet or keyboard sequences (e.g. “QWERTY”).

University will not be responsible for any loss of data from any IT resources located in the University or from the User’s own system, whether that content is protected by a user name and password, or otherwise.

D. Specific Responsibilities of Users:

Faculty, staff and students with authorized accounts may use the IT facilities for academic purpose, official purpose and for any other purpose so long as such use;

- does not violate law under IT Act 2000 of government of India.
- does not interfere with the performance of university duties or work of an academic nature.
- does not result in commercial gain or private profit other than that allowed by the university.

All Users must adhere to the following responsibilities:

1. Self-policing of passwords and access codes as set forth above. It is the user's responsibility to protect their account from unauthorized use by changing password.
2. Officials of the university are advised to use only official e-mail id issued by Head, UITS for official communication.
3. Downloading and installing of new software has to be done with the consent of the respective dean/in-charge. Installation of unlicensed software on GGS IP University facilities, or on individual machine connected to GGSIPU network is strictly prohibited.
4. Setting up of any facility requiring password transmission without permission of Head, UITS is strictly prohibited.
5. Users are advised to minimize the use of external storage backup devices, If essential, they must be used with prior permission and must be scanned for any viruses before using them.
6. It is forbidden to use e-mail and other network communication facilities to harass, offend, or annoy.

7. It is forbidden to send frivolous or academically unimportant messages to any group. Broadcast of messages to everyone in the system is allowed only for academic purpose and emergencies. Violation of this will result in immediate freezing of user's account's.
8. Any special accounts, if need to be set up for conferences and other valid reasons as determined by the GGS IPU authorities, must have a single responsible user.
9. Recreational downloads and peer to peer connection for recreational purpose are strictly banned in the university campus. Playing of computer games using IT resources of GGSIPU is strictly prohibited.
10. Users are expected to connect only to the official GGSIPU wi-fi network for wireless access. Setting up of unsecured personal wi-fi systems on GGSIPU network is strictly prohibited in accordance with IT act 2000.
11. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.
12. Display of offensive material (either on computer screens or through posters etc.) is strictly disallowed and serious action will be taken against offenders.
13. Any damage or theft of IT resources shall be dealt as per the disciplinary rules of the University. Users are responsible for Respecting and protecting the confidentiality, integrity, and availability of all University IT Resources.
14. BYOD (bring your own device) policy is followed in the University and are subject to the compliance of IT policy in terms of its usage.
15. Users are responsible for ensuring that all data and files that the User accesses, transmits, and/or downloads are free from any computer code,virus, file, or program which could damage, disrupt, expose to unauthorized access, or place excessive load on any computer system, network, or other IT Resource;
16. Users are required to report any security risk or code, file, or program, including computer viruses, Trojan Horses, worms, or any other malware that affects any IT Resource including any owned or operated by the User;
17. Properly backing up appropriate User systems, software, and data.
18. Switching off all IT resources after their use unless asked for otherwise.
19. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate.

Users of GGS IP University computing, networking and IT facilities are expected to abide by the IT Policy, which is intended to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve our right to access the networks to which it is connected.

E. Prohibited Uses of ICT Infrastructure

Users are prohibited from accessing or using the IT Resources in the following manners:

a) Initiating or participating in unauthorized mass mailings to news groups, mailing lists, or individuals, including, but not limited to, chain letters, unsolicited commercial email (commonly known as “spam”), floods, and bombs;

b) Seeking to, without authorization, wrongly access, improperly use, interfere with, dismantle, disrupt, destroy, or prevent access to, any portion of the IT Resources including User or network accounts;
c) Violating or otherwise compromising the privacy, or any other personal or property right, of other Users or third parties through use of the IT Resources;
d) Disguising or attempting to disguise the identity of the account or other IT Resource being used including "spoofing" resource addresses, impersonating any other person or entity, or misrepresenting affiliation with any other person or entity;
e) Using the IT Resources to gain or attempt to gain unauthorized access to networks and/or computer systems;
f) Engaging in conduct constituting wasteful use of IT Resources or which unfairly monopolizes them to the exclusion of others;
g) Engaging in conduct that results in interference or degradation of controls and security of the IT Resources;
h) Unless expressly authorized by the University in writing, exploiting or otherwise using the IT Resources for any commercial purpose;
i) Taking personal print-outs from official printers;
j) Engaging in computer crimes or other prohibited acts;
k) Intentionally or unintentionally violating any applicable local, state, federal, or international law;
l) Knowingly or negligently running, installing, uploading, posting, emailing, or otherwise transmitting any computer code, file, or program, including, but not limited to, computer viruses, Trojan horses, worms, or any other malware, which damages, exposes to unauthorized access, disrupts, or places excessive load on any computer system, network, or other IT Resource; and
m) Using any IT Resource, including email or other communication system to intimidate, insult, embarrass, or harass others; to interfere unreasonably with an individual's work, research, or educational performance; or to create a hostile or offensive environment.

F. Privacy

The University reserves the right to access, inspect, examine, monitor, intercept, remove, restrict, and take possession of all University owned and operated IT Resources, including but not limited to, electronic mail network connectivity, hard disks, printed media, devices, data, software, printers, voice mail, removable media, fax machines, scanners, computers, mobile devices, telephony equipment, connected devices, laptops, documents, and other files.

The University may exercise these rights for various reasons, including but not limited to:

- Ascertaining whether Users are using the systems in accordance with the IT Policy and other university guidelines;
- Preventing, investigating, or detecting unauthorized use of the University's systems;
- Ensuring compliance with applicable laws and regulations.

Users are expected and obligated to use such IT resources in a manner consistent with the purposes, objectives, and mission of the University and this policy.

Users should note that the University may also require back-up and caching of various portions of the IT Resources; logging of activity; monitoring of general usage; and other activities that are not directed against any individual User or User account, for protecting the University's IT Resources and systems, maintaining security and maintenance, or restoring normal operations of the IT Resources.

The University reserves the right to examine, use, and disclose any data or Content found on the University's IT Resources for the purposes of furthering the health, safety, discipline, legal rights, security, or intellectual or other property of any User or other person or entity. Information that the University gathers from such permissible monitoring or examinations may also be used in disciplinary actions. Such information may be disclosed to law enforcement officials when necessary.

G. University and Ethical Compliance:

GGS Indraprastha University shall provide IT services to all employees and students with a modern, fully networked computing and IT environment for academic and administrative use as specified as per their roles in the University system.

The Users are expected to fully comply with the standards and responsibilities of acceptable use of ICT Infrastructure, not specifically covered by this policy, as listed below:

- All applicable provisions of the University Code of Conduct, employee handbooks and agreements, student handbooks and other policies and procedures established by the undergraduate, graduate, and professional schools of the University;
- All application and/or software license agreements acquired by the University and its authorized units;
- The legal and educational standards of software use as published in the NASSCOM Code of Ethics

The University will periodically update this policy. By accessing and using the IT Resources, each User represents and acknowledges that he or she has checked and read this policy on a regular basis so as to be informed of any changes hereto. If any User does not agree to check the IT Policy for revisions on a regular basis, said User may not use the IT Resources. Changes to the policy are notified on the University Website from time to time.

For any suggestions, clarifications, grievances, kindly contact:

University IT Services Cell
DWS-412, 4th Floor, D-Block
GGS Indraprastha University
Sector 16-C, Dwarka, Delhi-110078
Phone: 011-25302746
Email: uits@ipu.ac.in