IT Security Policy for College Staff (Teaching and Non-Teaching)

Purpose

The purpose of this policy is to set terms and conditions, as well as standards and guidelines, for the acceptable uses of the IT services and assets provide to the college staff, contractors and visiting faculty. DES expects college staff, contractors and visiting faculty to become familiar with individual and institutional responsibilities to protect its electronic information.

Scope

This policy applies to all the users in the College, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

Policy

This IT Security Policy covers the following:
1. IT Assets
2. Password Control
3. Email
4. Internet and Wi-fi
5. Antivirus
6. Inventory
7. ERP System
8. CCTV
9. Data Backup

IT Assets

1. Employees should handle all the IT assets of DES properly and in a secure manner. This applies to desktops, laptops, printers and other equipment, applications and software, to anyone using those assets.

2. Active desktop and laptops must be secured if left unattended.

Principal,
D. E. SOCIETY'S
Kirti M. Doongursee College,
of Arts, Science & Commerce,
Dadar (W), Mumbai - 28.

3. Access to assets is forbidden for un-authorized personnel. Granting access to the assets involved in the provision of a service must be done through the approved Service Request Management and Access Management processes.

4. Users shall maintain the assets assigned to them in a responsible manner and not cause any damage to them.

5. The IT Technical Teams are responsible for maintaining and upgrading configurations. None other users are authorized to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.

6. Special care must be taken for protecting laptops and other portable assets from being stolen. Employees must be aware of extreme temperatures, magnetic fields and use of such devices in wet laboratories should be avoided.

7. Whenever possible, encryption technologies should be implemented in portable assets.

8. Assets (Laptops, desktops) storing sensitive information such as examination question papers must be password protected and it would be the responsibility of Teacher-In-Charges and Heads of the Department/Post Graduate programme Coordinators. The device also in turn should be password protected and should be left unattended.

Password control

1. All laptops and desktops must be protected with a strong password-based access control system.

2. Every user (teacher) must have a separate, private identity for accessing IT network services.

3. Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.

4. Password should be changed after every 90 days.

5. Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.

6. Writing down passwords on notepads or on sticky notes and storing it in personal mobile devices is forbidden.

7. Whenever a password is deemed compromised, it must be changed immediately.

8. Devices which are used in the laboratory should be password protected and for Access points in the laboratories, teachers should login through the firewall, if internet is being

used and should log out, once the use is over. This is specifically for using multiple devices in laboratories for teaching.

Email

1. Henceforth, email addresses issued by the organization shall be used for all official communication within the College and outside College for educational and research purposes only. (Use fergusson.edu and despune.org email IDs only).

2. All the assigned email addresses, mailbox storage and transfer links must be used only for business purposes in the interest of the College and DES.

3. Use of the College and DES resources for unauthorized advertising, external business, spam, political campaigns, and other uses unrelated to the College and DES business is strictly forbidden.

4. In no way may the email resources be used to reveal confidential or sensitive information from the outside College and DES. In unavoidable circumstances, confidential data information has to be encrypted or password protected before being sent.

5. Using the email resources of the College and DES for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.

6. Outbound messages from all users should have appropriate signatures at the foot of the message.

7. Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.

Internet and Wi-fi

1. Access to pornographic sites, hacking sites, and other risky sites is strictly forbidden and will be dealt as per existing IT laws.

2. Internet access is mainly for business purpose.

3. All internet traffic is guarded by firewall. The employees in no way shall tamper the firewall. Every teacher will be provided with single login and this should be protected again with a strong password of 8 characters.

4. Attacks like denial of service, spam, phishing, fraud, hacking, distribution of questionable material, infraction of copyrights and others are strictly forbidden.

Principal,
D. E. SOCIETY'S
Kirti M. Doongursee College
of Arts, Science & Commerce
Dadar (W), Mumbai - 28.

5. Use of social sites in the college campus by using college internet is strictly prohibited. Social media platforms created only for promotion of college activities will be allowed to access through college internet.

6. Copyright Infringement-Any download using the service that will infringe a copyright of a material, audio, video or document is totally prohibited and will be subject to disciplinary action depending on the number of offenses

Data Backup

Data Backup is the responsibility of each user and back up has to be taken on College/DES approved shared locations. If backup is taken on pen drive or hard disc, it should be encrypted.

Antivirus

All windows computers and devices with access to the College and DES network must have an antivirus client installed, with real-time protection. Devices which store important college information and data will be protected by the antivirus for which there is separate budgetary provision.

Inventory

1. All items of equipment to be brought under control shall be identified by a serial number affixed to each item.

2. Equipment control records shall be maintained for each item of equipment identified by a serial number and an appropriate stock registration number and should be duly entered in the College Asset Register.

3. Periodic physical inventories, at least once annually, shall be taken of all items of equipment placed under serial number control.

ERP system

1. ERP system can be accessed from mobile and PC. Employees will not share login Id or password with anyone.

2. The email Id and the contact details provided as input to the ERP system have to be up to date.

3. Teachers should avoid using the ERP system from any cyber café. In case of unavoidable circumstances, after ERP system is accessed from any cyber café, cache and local copies of any documents should be cleared.

Principal,
D. E. SOCIETY'S
Kirti M. Doongursee College,
of Arts, Science & Commerce,
Dadar (W), Mumbai - 28.

CCTV

1. The College campus is monitored by CCTV for stakeholder security. None shall tamper it in any way.

IT Security Policy for Students

Purpose

The purpose of this policy is to set terms and conditions, as well as standards and guidelines, for the acceptable uses of the IT services and assets by the *Fergusson College (autonomous)*, students. *Fergusson College (autonomous)*expects students to become familiar with individual and institutional responsibilities to protect its electronic information.

Scope

This IT Security Policy covers following IT Services and assets:
1. Laboratory computers
2. Wi-fi connectivity to devices
3. ERP system access
4. LAN access
5. BYOD
6. CCTV
7. Email and Teams
8. Use of social media
9. Netiquette for Online Education

Policy

1. Laboratory computers

   Students will in no way damage or tamper the laboratory computers. Laboratory computers shall be used only for laboratory practical assignments and for storing data pertaining to research projects.

2. Wi-fi and LAN connectivity to devices

Principal,
D. E. SOCIETY'S
Kirti M. Doongursee College,
of Arts, Science & Commerce,
Dadar (W), Mumbai - 23.

Wi-fi and LAN connectivity will be available as is. Valid username and password obtained from Computer Services Office/ respective department/teacher is required when accessing wi-fi and LAN network and shall be used for academic and research purpose only. Internet services provided will be guarded by firewall. Firewall policies will have to be adhered to. Wi-fi or LAN connectivity is not supposed to be used to access any unauthorized content or hack any internal or external systems or sites.

3. ERP system access

ERP system can be accessed from mobile and PC. Students will not share login Id or password with anyone. The email Id and the contact details provided as input to the ERP system have to be up to date. Students should avoid using the ERP system from any cybercafé. In case of unavoidable circumstances, after ERP system is accessed from any cybercafé, cache and local copies of any documents should be cleared.

4. LAN Access

Unauthorized devices shall not be connected to the LAN. Devices shall be connected to LAN after obtaining firewall credentials from the college.

5. BYOD

Physical security of the student's personal devices is not the responsibility of *Fergusson College (autonomous)*. Using the *Fergusson College (autonomous)*wi-fi or LAN connectivity, no viruses should be infused or spread. If the student's device is to be used for any laboratory work, prior permission from the Teacher-In-Charge/ Head of the Department should be taken.

6. CCTV

The College campus is monitored by CCTV for the students' security. No student shall tamper it in any way.

7. Email and Teams

Email addresses issued the college for attending online classes shall be used responsibly. Sending SPAM emails is strictly prohibited. Students attending online

classes using Teams shall not disturb online classes. They will follow instructions provided by the teachers. Students will not use the platform for bullying or harassing other students.

8. Use of social media

Students should not use any social media platforms for posting defamatory posts regarding fellow students, neither troll them nor bully them, this will amount to ragging activity and it will be dealt as per UGC regulation.

9. Netiquette for Online Education

The present situation of pandemic has made online education/ communication mandatory and has become part of our lives. Online education will be provided through Microsoft team's platform which is official platform for academic communication. However, certain netiquettes for online education need to be followed, which are as follows:

a) Use clear, courteous, concise and respectful language with your fellow classmates and teachers

b) Do not use abusive language and avoid using slangs as all lectures/interactions are recorded

c) Do not share online education material outside the College without prior permission of the teacher/ coordinator, similarly do not post inappropriate material.

d) Avoid sharing personal / confidential information of yours and others.

e) Be attentive during online classes and submit/share your assignments in time.

f) Read all updates communicated to you through ERP and MT platforms.

g) Keep visiting college website for important notices and updates especially with regard to examination/ assessment.

h) Communicate to your teacher in case of any difficulty, in time.

i) Make sure your identification is clear during online classes/ interactions.

j) Do not share your user ID and password which could put your safety or security at risk.

Principal,
D. E. SOCIETY'S
Kirti M. Doongursee College,
of Arts, Science & Commerce,
Dadar (W), Mumbai - 28.

Student User Agreement

The use of the IT Service for the following unlawful activities is prohibited:

1. Sharing Username and Password

    Sharing username and password to anyone is unacceptable. User who provides such information to others to gain internet access will be removed from the network permanently.

2. Copyright Infringement

    Any download using the service that will infringe a copyright of a material, audio, video or document is totally prohibited and will be subject to disciplinary action depending on the number of offenses.

3. Spamming and Invasion for Privacy

    Sending of unsolicited bulk and/or commercial message over the internet using the service or using the service for activities that invade another's privacy is prohibited.

4. Private Commercial Purpose

    Using the service for personal gain; for example, by selling your username and password to others, or by performing work for profit with College (autonomous) resources in a manner not authorized by the College.

5. Defamatory or Abusive Language

    Using the service to transmit, post, upload, or otherwise make available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another is prohibited.

6. Hacking

    Accessing illegally or without authorization to computers, accounts, equipment, or networks belonging to another party, or attempting to penetrate security measures of another system is prohibited.

Principal,
D. E. SOCIETY'S
Kirti M. Doongursee College,
of Arts, Science & Commerce,
Dadar (W), Mumbai - 28.

7. Pornography

Student will not visit sites that are considered obscene. The college prohibits users from using its service to send sexually oriented images or messages. In the event that a student disregards this policy and continually visits unauthorized sites, it will be grounds for internet access after a warning has been issued to that user.

8. Supervision and Monitoring

The College reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including students' login sessions to determine if a user is violating any agreement mentioned above. The College has the right to determine which uses constitute acceptable use and to limit access to such uses. The College has the right to limit the time of access and priorities among competing acceptable uses. The College also reserves the right to view private files that have been downloaded to check for the propriety of downloaded files and monitor bandwidth usage.

9. Virus attack
Any personal devices that are to be connected with the College wi-fi network should be free from virus.

10. VPN Access
College students will not use any VPN or any proxy server.

11. Unauthorized copy of software
Students are not allowed to make an authorized copy of any legitimate   software that belongs to the College.