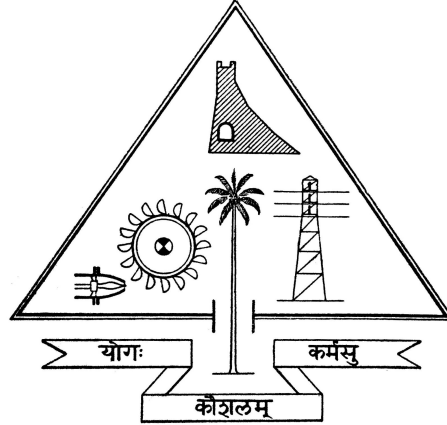# Government Engineering College
Thrissur

Internet Usage and Security Policy

Common Computing Facility

Internet Usage and Security Policy

1. Overview

Internet connectivity presents with new risks that must be addressed to safeguard the facilities, vital information assets. Access to the internet will be provided to faculties, staffs and students (further referred as **users**) to support academic activities and only on and as needed. Access to the Internet by users that is inconsistent with academic needs results in the misuse of resources.

2. Purpose and Scope of the document

The purpose of this policy is to define the appropriate uses of the internet by the students, faculties and staffs of the Government Engineering College, Thrissur.

This policy applies to all internet users (Faculty, Technical staff, Administrative staffs, Contract/Temporary staffs and Students and Research Scholars) who access the internet facility provided by the GEC Thrissur through Wired or WiFi networking. The internet users are expected to be familiar with and to comply with this policy.

3. Internet Access Request and Approval

Internet access will be provided to users for their academic needs only and they restricted to access the contents under the academic category only.

As part of the Internet access request process, the employee is required to read the Internet usage and Security Policy. The user must sign the declaration in the application that they understands   and   agrees   to comply with the policies. Users not complying with these policies could be subject to disciplinary action.

3.1. Apply Procedure

- **Students**: All the students are required to submit and internet access request form to the CCF through the staff advisor.
- **Faculty/Staff**: Faculty and staff members have to submit their duly signed request to the CCF for getting the access.

3.2 Approval and Access

Applications will be examined and approved at CCF and a username and password will be given to the user. All the activities using this user id is logged at the CCF and the user is solemnly responsible for the activities associated with their user id.

3.3 Removal of Access
Internet access will be discontinued upon completion of study of student, completion of contract, transfer of faculty/staff, <u>or any disciplinary action arising from violation of this policy</u>.

The privileges granted to uses and continue sly monitored and may be revoked at any time if it is no longer needed by the user.

4.   Usage Policy

4.1.   General Guidelines

- Internet users of GEC Trissur shall comply with applicable National/State/Cyber laws and rules and policies of GEC Thrissur. Examples of Rules and policies include, the laws of privacy, copy right, trade mark, obscenity and pornography. The IT act 2000 which prohibit hacking, cracking, spoofing and similar activities.
- According to the GEC policy, the tethering/hotspotting of internet connection is liable for deactivating the connection.
- Users will be required to obtain necessary authorisation before using college connectivity.
- Users will also be responsible or any activity originating from their account
- Accounts and passwords should not under any circumstances be used by any other persons other those to whom they have been assigned by CCF.
- In case of unauthorized use of account is detected or suspected, the account owner should change the password and report the incident to CCF.
- Uses shall not use college network and connectivity to get unauthorised access to remote computers which may damage the operations of GEC Network.

4.2.   Security and Privacy

- Uses should engaging safe computing practices by establishing appropriate access restrictions for their account and computing devices, guarding there password and changing them regularly.
- Users should note that their uses of College connectivity are not completely private. As part the security measures, all the activities are logged and monitored at CCF.
- The College, in its discretion may disclose the results of any such general or individual monitoring including the contents and records of communication to the appropriate authorities or law enforcement agencies and may use those results for disciplinary procedures.

4.3.   Prohibited Downloads

The following downloads are specifically not allowed on computers unless approved in writing by CCF.
- Any peer to peer file sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications – called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer.
- Any third party personal antivirus or firewall: Since adequate security has already been provided for on all machines via pre-defined firewall rules, third party firewalls may interfere with these rules thus endangering the network.
- Any Proxy servers, private fire wall, tunnelling software, connectivity sharing software
- Hacking tools of any sort: The use of any such tools on college network is strictly prohibited.
- Games & Movie trailers or previews
- Any other copyrighted content/materials/software which are not appropriate to the user

4.4. WiFi Policy

- College WiFi ('**GECTCRWIFI**') is available in the whole campus and hostels. Wifi will not be available at hostels during class hours.

- The access to college Wifi restricted to registered users. The one who wants to avail the WiFi facility, has submit an application in the prescribed format and the personally bring the device to register at CCF.

- The access to college Wifi is restricted to the registered device only. Usage of college Wifi in an unregistered device by spoofing/tethering will be treated as violation of this policy.

- Even if the access id is different, the registered Wifi user is the sole responsible person for all the communications originated from the registered device.

4.5. Enforcement

- Users found violating this policy may be denied to access to the GEC network for a minimum period of six months and may be subject to other penalties and disciplinary action.

- The GEC network admin may suspend, block or restrict the access to an account, when it reasonably appears necessary to do so in order to protect the security, integrity or functionality of the network

- Suspected violations of applicable laws may be referred to appropriate law enforcement agencies

- Alleged violations will be handled through GEC Thrissur disciplinary procedures applicable to the user

5. Disclaimer

- GEC Thrissur reserves the right, without notice, to limit or restrict individual's use and to inspect, copy, remove or otherwise alter any data, file or system which may undermine the authorized use of any computing facility or which is used in violation of GEC Thrissur rules and policies.

- GEC Thrissur also reserves the right periodically to examine any system and other usage and account activity history as necessary to protect its computing facilities.

- GEC Thrissur disclaims any responsibility for loss of data or inference with files resulting from its effort to maintain security and privacy.

- GEC Thrissur reserves the right to amend these policies at any time without prior notice and to take necessary action to comply with applicable laws.

Government Engineering College – Thrissur

General Do's	General Don'ts
1. Do respect the rule "That which is not expressively permitted is prohibited".	1. Do not download content from Internet sites unless it is related to your work.
2. Do use the internet only for academic related matters	2. Do not make any unauthorized entry into any computer or network.
3. Do check the information you access is accurate, complete and current.	3. Do not represent yourself as another person. Do not share your password.
4. Do respect the legal protections to data and software provided by copyright and licenses.	4. Do not use Internet services to transmit confidential, political, threatening, obscene or harassing materials.
5. Do inform the CCF in case of any unusual occurrence.	5. Do not attach/transmit files through email which contains illegal/unauthorized materials.
6. Do contact the CCF in case of any Internet related problems.	6. Do not use GEC Thrissur network for Peer to peer file sharing.
7. Do clean the browser history and cache periodically.	7. Do not download any image/video/file which contain pornographic, racist, violence or any illegal activity.
8. Do sign off from captive portal when you are not using Internet or leaving the system.	8. Do not use Internet services to download movies/previews/Games.