Internet/IT Policy at MCF dated 05.08.2020

Deployment of thin clients for secured Internet access:

- Secured ID based internet access.
- Customary Internet access facility for all the functionally designated Officials.
- Internet access facility for other officials with the approval of Director on case to case basis.

General Internet Browsing – Best Practices

Browser Security

- Always use updated anti-virus, Operating System and applications and browser.
- Use a web browser with sandboxing capability (like Google chrome, safari, etc.). Sandboxing usually contains malware during execution.
- Make a habit of clearing history from the browser after each logout sessions.
- Delete Windows “Temp” and “Temporary Internet files” regularly.

Downloading

- Download software from trusted source or trust worthy websites only. Do not click links to download anything you see on unauthorized sites.
- Be conscious of what you are clicking on/downloading.
- Some pop-ups have what appears to be a close button, but will actually try to install spyware when you click on it.
- Remember that things on the Internet are rarely free. “Free” Screensavers, etc. generally contain Malware.
- Be wary of free downloadable software – There are many sites that offer customized toolbars or other features that appeal to users, which are likely to have backdoors.
- Scan all the files after you download whether from websites or links received from e-mails.
- Do not click the link or file and let it start download automatically, download the file and save where you want to save and then run on the application.
- Neve download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favourite search engine to see anyone posted or reported that it contains unwanted technologies.

- Be extremely careful with file sharing software. File sharing opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk serious legal consequences.

Personal Security

- Be wary of storing personal information on Internet.
- Do not store any information you want to protect on any device that connects to the Internet.
- Avoid all cloud services (Dropbox, iCloud, Evernote, etc.) that are based outside India.
- Avoid using services that require location information.
- Remember search engines track your search history and build profiles on you to serve you personalized results based on your search history.
- Never exchange home and office work related contents.
- Avoid posting of photos with GPS coordinates.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.

Other measures

- Frequently check unusual folder locations for document (.doc, docx .xls, .xlsx and .def) file extensions (in search options, select advanced search options, make sure you checked “Search System folder”, “Search hidden files and folders” and “search subfolders”)
- Avoid Internet access through public Wi-Fi.