No. H2/65374/09
Police Headquarters,
Kerala, Thiruvananthapuram
Date: 06/10/09

Circular No. 40/09

Sub: - Police Department- Internet Usage and Email Communications- Instructions Issued.

01. Considering reduction in costs, speed of delivery and ease of use , it is desirable that the use of E-mail be increased in Police Communications. This will enable Police to perform statutory duties with minimum wastage of time and interpose effectively in situations which warrant Police intervention in the prevention and detection of crimes. Further, E-mail communications will result in savings in resources such as paper, stationery, expensive ink toners, postage etc. in addition to this , wastage of human resources on dispatch duties expenditure in, fuel, time and energy can be avoided by resorting to this simple, cost effective and instantaneous method of communication. The IT Act 2000 grants legal sanctity to electronic records and provides statutory support to the record management in an electronic environment. It also permits retention of records in electronic form.

02. Considering the above advantages, a standard methodology for use of E-mail in Police Communications is necessary.

03. Police Offices having Internet Connectivity should use E-mail communication for all routine matters unless otherwise required to use other methods for maintaining confidentiality of communications or for ensuring guaranteed identification of authority.

Since the Government has issued all officers and offices with e-mail identities the onus is upon each individual officer to ensure that his e-mail and the mail of his office is opened regularly and mails received acted upon or responded to promptly. E mail should be treated as equivalent to a letter on paper.

ADMINISTRATION:-

04. The officers-in-charge are responsible for the integrity and authenticity of the E-mails and Attachments they are sending. All E-mails from the concerned officer are summarily presumed as emanating from the concerned officer. Therefore, Password confidentiality is the responsibility of the officer in charge of the Computer System. To help ensure the integrity and authenticity of the E-mail messages officers, must not share their password(s) with others.

05. Forgetting passwords or losing them or negligent conduct with password leading to misuse of e-mail accounts will be deemed dereliction of official duty. In case a password is forgotten, the concerned officer may inform the matter to the concerned IP Tele in writing. The IP Tele through proper channel (SP Tele and IGP SCRB) will obtain a new password for the

E-mail from the System Administrator at KSITM. Till the time the new password is obtained, all the official E-mails can be sent from the concerned CI office/ Superior Officer's E-mail address.

06. Officers on transfer are responsible for handing over the password to the incoming officers. Officers after taking over charge are expected to change the password on the same day. Under exceptional circumstances, if there is no officer to take over charge, the password may be handed over to the immediate Superior Officer in a sealed cover. The relieved officer may hand over all the official E-mail communications and Electronic records to the relieving officer.

07. One authorized person preferably the Station Writer/Circle Writer/CA may be designated in each Police Station or office for maintaining access control to the official E-mail facility.

RECORD KEEPING:-

08. E-mail messages are records and are to be managed accordingly. Rules of disclosure of E-mail are the same as for paper records. Officials concerned are obliged to provide access to E-mail messages in the event of legal dispute or as part of a request under the Right To Information Act. This can include E-mail messages on hard copy, hard drives or on networks.

09. Folders in the computer will act as substitutes for Paper File Bundles. Communications received on the same subject can be kept together in a Folder in the E-mail account itself. In addition to that, the official E-mails can be stored for ready reference, without net connection, on the Desktop of the Computer in a Folder Called "Received E-mails:" Then this Folder can have sub-folders for different groups of subjects or different subjects. Each such sub-folder can have further sub-folders for communications with regard to a specific matter relating to the subject or with regard to group of subjects forming a sub-group within the subject. There is practically no limit to the possible number of folders or subfolders. Therefore on the Desktop of the Computer received E-mails for official purpose can be permanently stored and should be periodically saved on a CD or a back-up system to guard against permanent accidental loss. (Alternatively, regular software packages which allow storing of E-mails in the Computer itself may be used to achieve the same purpose or ready reference in the computer itself without going online.)

10. The same system can be used for Sent E-mails also for record purposes.

11. The subjects on which the Folders may have to be uniformly maintained will be separately given in an Executive Directive. Additional sub folders can be maintained within any folder. Additional folders can be made depending on local conditions.

12. In addition, on the computer desktop a "Register of Received E-mails" and "Register of Sent E-mails" may be maintained, with column headings given at present in the "Inward Register" and "Dispatch Register". For this the Spreadsheet format may be used. In addition to the present columns, there should be another column for the "location" inside the computer of the copy of the originally received mail or of the sent mail as may be applicable.

13. All users should take a CD Backup of all the E-mails every week, updating the CD from week to week. The CD be stored after entering the datas involved on the CD in a clean CD Box. Once the CD is full, another CD may be used.

14. A Central Archive of E-mails will be maintained in Telecommunication Head quarters with DySP (Communication and Training) in the form of CDs, both subject-wise and year-wise.

15. All E-mails will be presumed as sent or received as the case may be on the appearance of delivery report to the sender. The Sent mailbox will contain the details of sent E-mails.

16. A register has to be maintained outside the computer system in a hand written Register as a ready reference of official E-mails received and sent. The Proforma will include Sl.No., Date and Time, Sender, Receiver, Subject and Attachments. The system of maintaining such a register will be reviewed on 1.1.2011 and dispensed with if no longer necessary due to greater familiarity of users with the digital system of record keeping.

17. All the communications/feedback received through the official website will be treated as 'received tappal' and will be processed accordingly. However spam or unnecessary mail may be deleted by the officer immediately.

NEW E-MAIL ID:-

18. All new Police stations and Police offices need new E-mail Ids. A new E-mail Id can be obtained by the concerned officer by addressing the SP Telecommunication.

MANNER OF USE OF INTERNET CONNECTVITY AND E-MAIL:-

19. Users are prohibited from visiting undesirable sites and resorting to general web browsing. Use of internet should be for official purpose only.

20. No Private communication and Internet surfing for private purposes is permitted at government expense through the official Computer Systems, Networks or Wifi facilities.

21. All officials are responsible for composing, using, communicating and sharing E-mail messages in accordance with Government guidelines. They will maintain E-mails as official records to meet legislative and departmental requirements.

22. All E-mails carry a subject field. The matter entered in this field appears in the mail box of the recipient. It is important that the subject matter indicates the type of content in the mail for easy comprehension and classification. The maximum length allowed for the subject field is 55 characters. So be brief. A list of standard abbreviations to be used in subject field or name field will be separately issued as an Executive Directive.

23. The Police Stations and Officers may use intermediate e-mail clint softwares which enable swift exchange of E-mails within a short period and storage of the same for reading and replying during off line time. This will save precious Internet time.

24. All computers on which e-mail is accessed should have antivirus software with capability for automatic scanning of incoming mail and attachments. All E-mail attachments must be Virus-scanned and opened only if no threat is detected by the Anti-Virus software.

25. Users may maintain an Address Directory/E-mail Directory in their respective E-mail accounts for effective time management.

26. E-mails and Attachments may be brief and to the point. The size may not normally exceed 500 KB including attachments etc. Hyper Links instead of large attachments may be resorted to, to save download time and to ensure speed of communication. Standard fonts like Ariel, Courier, Verdana, and Tahoma may be used instead of flowery and calligraphic fonts. The font size may normally be between 12 to 14 points.

27. All periodical reports and Special reports can be sent through E-mail. For State wide periodicals, IGP SCRB and SP PCC will standardize the format of the periodicals. In other cases, the authority asking for the information must prescribe the digital format in which the data is to be sent. Such standardization is essential for digital calculations and compilations. While selecting addressees or recipients of copies of e-mails sent care should be taken to see that mails and replies are sent only to those who are to get or receive the information by virtue of their official responsibilities. Copies of mails or replies should not be addressed / forwarded to officers without any specific purpose just because they are in the chain of command.

TIMING OF USE:-

28. All Police Stations, CIs and DySPs, who are provided with Internet facility, may open the Internet at least once in 12 hours. If a sender wants immediate attention of the recipient to a mail he has dispatched, he may telephonically request the recipient to open the E-mail.

29. Internet time must be efficiently used. The use of internet by all the officials at a single point of time will over burden the Mail Server. To prevent the related problems, it is prudent to use Internet during staggered and pre-notified time schedules. S.P. Telecom may suggest suitable staggering of times as may be appropriate depending on the capacity of the server.

NEED FOR VERIFICATION BEFORE ACTION:-

30. E-mail communication shown as coming from the Superior officers is insufficient to authorize officers for resorting to arrest or custody or expenditure from the exchequer or any coercive action. This is because our network is not a secure network. Verification of some sort may be done before initiating any such action.

31. Incoming E-mails may include petitions, informations etc. Such E-mails may be verified on the ground and then acted upon. However, such verification may be completed at the earliest assuming that the E-mail is genuine. Immediate registration of FIRs based on E-mails directly received from unknown persons is not advisable without some preliminary verification. The procedure followed when telephonic information is received regarding a cognizable offence is to be emulated. That is, a preliminary verification on the ground may be resorted to. If there is reason to believe authority of the communication, then FIR may be registered on the basis of the E-mail.

GENERAL:-

32. Wireless Communication, Telephonic communication, Written communication and CoB are the various modes of communications available in case of breakdown of E-mail communication. Officers may use the fastest mode of communication possible in case of contingencies.

33. In case of breakdown of E-mail communication in a particular computer system, the Computer System of the immediate Superior officer or the nearest police station can be used. However, the problem may be rectified with the help of maintenance staff.

34. Printing should not normally be resorted to unless the communication is meant for another Department or a Court of Law or has to be acted upon by registering itas a petition / FIR etc

35. All traditional wireless transmitted communications may be sent through both E-mail and Wireless telecommunication till 31st December 2009. All E-mails may be notified by wireless or by phone till 31st October 2009. The sender will give a brief wireless message alert or telephone alert with the subject and nature of priority only.

36. No secret messages and classified information shall be sent through E-mail. The conventional system of using Wireless Telecommunication through Cipher may be resorted to ensure confidentiality.

37. Some essential general guidelines while using Internet and E-mail facilities are given in Annexure.

38. Inspector General of Police SCRB will be in overall charge of E-mail and Internet Services. He will be assisted by SP (Tele) in the matter of maintenance and upkeep of hardware and by SP (Computers) in the matter of stock of computer hardware and maintenance of software.

S/d

DIRECTOR GENERAL OF POLICE,
KERALA

Annexure

Internet Usage – General Guidelines

1. Protect confidential and sensitive E-mail content by managing your in- and out-boxes or by installing encryption software.
2. Be careful with your personal information, and do not give information such as your family's address, phone number, credit card or calling card numbers etc. over the net.
3. Respect the privacy of other users on the Internet.
4. Be careful when you copy ("download") programs from the Internet.
5. Do be aware of file size. Plain text messages take up the least space and shortest time to transmit. Avoid attachments, but if you must send an attachment, check the file size before transmission to avoid overloading your recipient's inbox and warn them it's coming.
6. Organize your E-mail into folders.
7. Use discretion when printing E-mail messages. Minimise printing and paper copies.
8. Reply to original messages. This helps the recipient understand the context of the reply.
9. Use the auto-signature option in Exchange. This saves you from typing your name and other contact info (E-mail, phone, and fax) for every message.
10. Do use plain text instead of html messages.
11. Do be careful of who is receiving your mail. Make sure you have the correct person. Keep your address book updated.
12. Do be neat; check spelling and grammar using spell check function. Your E-mail correspondence reflects your professionalism, competence and ability to use the technology appropriately.
13. Do use the Subject line creatively to summarize content. The subject line encourages your contact to read your E-mail right away.
14. Do save copies and get receipts for critical messages. If the message is important, get an electronic receipt and send yourself a copy (and file it).
15. Use all courtesies that is normally used in paper mail in e-mail communications also such as in salutations and language.
16. Don’t give your user ID or password to another person or wrote it down at openly at obvious places.
17. Don't make copies of any copyrighted material.
18. Don't give out passwords or credit card numbers online.
19. Don't tamper with or hack into someone else's computer. That is a serious crime.
20. Don't allow E-mail attachment from an unknown sender to be opened; it may contain a virus.
21. Don't put something in an E-mail message that you would not want read by everybody.
22. Don't send an E-mail without a meaningful subject.
23. Don't send and receive attachments without scanning them for viruses.
24. Don't use office E-mail for personal use.
25. Deleting a message does not absolve you of your responsibilities in the communication. So initiate action wherever necessary. Remember that the server contains records of all messages send and received.

****