Internet/DCN Acceptable Use Policy for the
U.S. District Court, Eastern District of New York

CONDITIONS, RULES AND ACCEPTABLE USE AGREEMENT

The United States District Court, Eastern District of New York and the Clerk of Court (the "District"), have actively pursued making advanced technology and increased access to research opportunities available to our staff. We believe this computer technology will help serve the Court by allowing staff to access and use information sources from distant resources, communicate and share information with individuals or other groups, and significantly expand their knowledge base. Users have access to both the Judiciary's Intranet (the DCN) and the Internet (collectively known as the "Network").

PROPER AND ETHICAL USE

With technology, staff must understand and practice proper and ethical use. All staff and interns/students must read and agree to this policy statement regarding procedures, ethics and security involving use of the Network before receiving an account name and password in order to use the system. The use of the Network is a privilege, not an entitlement. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of that privilege. The Clerk of Court, under this agreement, is delegated the authority to determine appropriate use and may deny, revoke, suspend or close any user account at any time based upon determination of inappropriate use by any account holder or user.

CONDITIONS AND RULES FOR USE:

1. Acceptable Use

The purpose of the Network is to facilitate communications in support of research and other Court functions by providing access to unique resources and an opportunity for collaborative work. To remain eligible as a user, the use of your account must be in support of and consistent with the objectives of the District. Access to the Network is made possible through the DCN and an appropriate provider as designated by Office of the Clerk of Court at its sole discretion. The Office of the Clerk of Court, all staff and other users of the Network must comply with existing rules and Acceptable Use Policies, which are incorporated into this document, and are available from the District as well as any national policy as put forth by the Administrative Office of the US Courts.

Employees accessing the Internet must adhere to the same code of ethics that governs all other aspects of judiciary employee activity.

1. Employees may not use the Internet for purposes other than authorized activities.
2. Only those employees specifically granted Internet access may use that access. Authorized employees are not to share this capability with anyone in any way.

2. Inappropriate Uses of the Internet

Judiciary employees should use government equipment (including that used to access the Internet) for official purposes only. Since no two employees will use the Internet in the same way, it is necessary for each user to exercise individual responsibility and judgment in the use of these services. Users should recognize that, as with other government provided resources, inappropriate, wasteful or illegal use can lead to disciplinary action.

Employees are specifically prohibited from using the Internet for the following purposes:

a. Sending data files or mail over the Internet that contains any discriminatory statements that malign any race, creed, color, sex, or sexual preference.
b. Making unauthorized commitments or promises of any kind that might be perceived as binding the government.
c. Sending data files or mail over the Internet that deal with ongoing investigations or litigation. The Internet is not a secure means of transmission and can cause a case or investigation to be compromised should the data be captured and read by an unauthorized party.
d. Sending data files or mail over the Internet that could reflect poorly, or cause embarrassment to the judiciary.
e. Taking part in Internet discussion forums that are not associated with official government business.
f. Posting opinions on the Internet to forums that are personal in nature.
g. Pursuing or researching matters that are not connected to official government business.
h. Using the network connection for commercial purposes or private gain; this includes using for product advertisement.
i. Using the network for illegal activities.
j. Transmitting any material in violation of any United States or state Regulation. This includes, but is not limited to, threatening or obscene material, or material protected by trade secret.
k. The use of peer-to-peer file sharing (i.e. bit torrent, gnutella, etc.) and instant messaging (Yahoo, Microsoft, AOL) for communicating with persons or entities outside the judiciary's private data communications network is prohibited. These programs pose extraordinary security risks to the judiciary's information technology infrastructure and will, in accordance with the policy adopted by the Judicial Conference, be blocked at the Internet Gateways until such time as the security risks posed by their use can be eliminated." IT Security Policy [2006-2]
l. Judiciary employees should only participate in chat rooms (i.e. WebEx) when directly relevant to their official duties and responsibilities. When participating in a chat room, employees should not inadvertently give the impression of articulating official judiciary policy or positions.

Improper use or distribution of information is also prohibited. This includes copyright violations such as software piracy. The judiciary may incur a legal liability for unauthorized copying of files or software even if the copy is used for official business. Employees should show respect for intellectual property and creativity by giving appropriate credit when files or portions of files are used while carrying out official duties. Employees should be mindful of procurement sensitive information and should not transmit it over the Internet. Employees should refrain from any practices which might jeopardize the judiciary's computer systems and data files, including but not limited to virus attacks, when downloading files from the Internet. Any downloaded files should be scanned for viruses. Employees are advised to not propagate viruses by transmitting files from the Internet to other users without first scanning them for viruses.

These guidelines apply to all Internet services accessed using computer resources of the judiciary. These services include but are not limited to: electronic mail, Web browsers, List Servers, Telnet, Remote Desktop Protocol (RDP) and File Transfer Protocol (FTP). Employees who are authorized to use these services must make sure that they use the Internet safely and productively, and not in any way that could compromise the interests of the judiciary. Access to the Internet is possible through the DCN. As part of the security system of the DCN's Internet gateway, a log is kept by the AO of all Internet activity passing through the DCN. This log is monitored at the gateway location for improper use. In addition, if an individual accesses an Internet site or sends an electronic message through the DCN's Internet gateway, the fact that this activity originated from the United States Courts will be known by the receiving site or party. Inappropriate access could therefore be an embarrassment to the judiciary

3. Electronic Mail

Any employee with a Lotus Notes account may use that account to send and receive Internet electronic mail provided that they follow the *acceptable use* provisions outlined in this section. Contact the Automation Department for directions on how to use Lotus Notes to send an electronic mail message over the Internet. It should be noted that Internet mail is not secure. Messages can be read or broadcast without the knowledge or consent of the author. Users should not expect the messages they send or receive via the Internet to be private. Internet mail is also unreliable. Delivery and delivery times are not guaranteed due to unpredictable intermediary system and network outages and slowdowns. Users should not rely on Internet mail for time-sensitive communications or guaranteed delivery. Also, any attachments to a message may not be readable by the receiving party.

Messages with large attached files, e.g. documents that include graphics, music, or messages sent to large numbers of recipients are discouraged. These messages may overload the system causing a failure. If there are work-related needs to transmit such messages, the sender should contact the Automation Department for advice on the best way to accomplish this.

With Internet mail you can subscribe to a variety of newsgroups, list servers, and other sources of information. These are potentially valuable information tools but their overuse will also increase network congestion on the DCN. Users should take this into consideration before subscribing to such services and should "un-subscribe" to any that are found to be no longer useful.

Checking personal E-Mail accounts could bypass virus scanners on the judiciary's mail servers, raising severe security risks locally and judiciary-wide. - IT Security Policy [IRM-2006-1]

It is not appropriate to use government systems to send or receive E-Mails containing greeting cards, political statements, jokes, pictures, and other items of a personal nature. Chain letters or other unauthorized mass mailings regardless of the subject matter, likewise are inappropriate.

4. Monitoring

The District reserves the right to review any material on user accounts and to monitor fileserver space in order for the Clerk of Court to make determinations on whether specific uses of the Network are inappropriate. In reviewing and monitoring user-accounts and fileserver space, the District shall respect the privacy of user-accounts. Users are hereby notified that messages over 90 days old may be automatically cleansed from the system and are encouraged to archive mail. Instruction on the procedure is available from the Automation Department.

5. Network Etiquette

All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

Be polite. Do not be abusive in your messages to others.
Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
Do not engage in activities that are prohibited under state or federal law.
Do not reveal your personal address or the phone numbers of colleagues.
Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities and may result in the loss of user privileges.

Do not use the network in such a way that you would disrupt the use of the network by other users.
All communications and information accessible via the network should be assumed to be private property.

6. No Warranties

The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, no-deliveries, mis-deliveries, or service interruptions caused by the District's negligence or by the user's errors or omissions. Use of any information obtained via the Network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they obtain, and consider how valid that information may be.

7. Security

Security on any computer system is a high priority, especially when the system involves many users. Users must never allow others to use their password. Users should also protect their password to ensure system security and their own privilege and ability to continue to use the system.

If you feel you can identify a security problem on the network, you must notify a system administrator. Do not demonstrate the problem to other users.

Attempts to log on to the Network as a system administrator may result in cancellation of user privileges.

Any user identified as a security risk for having a history of problems with other computer systems may be denied access to the Network by the District.

8. Vandalism and Harassment

Vandalism and harassment will result in cancellation of user privileges. Vandalism is defined as any malicious attempt to harm, modify, and destroy data of another user, Internet, DCN, or other networks that are connected to the EDNY network backbone. This includes, but is not limited to, the uploading or creating computer viruses.

Harassment is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted mail.

9. Encounter of Controversial Material

Users may encounter material which is controversial and which users may consider inappropriate or offensive. However, on a global network, it is impossible to control effectively the content of data and an industrious user may discover controversial material. It is the users' responsibility not to initiate access to such material. Any decision by District to restrict access to Network material shall not be deemed to
Impose any duty on District to regulate the content of material on the Network. All web activity is logged and is available for review by management.

10. Installation of Unauthorized Programs

Users may not install or cause to be installed unauthorized software. Likewise, users may not send nor may cause to send email messages that cause harm to the Network.

PENALTIES FOR IMPROPER USE:

1. Any user violating these rules, applicable state and federal laws or District rules are subject to loss of network privileges and other District disciplinary options.

2. In addition, pursuant to New York State law, any unauthorized access, attempted access, or use of any computing and/or network system may be a violation of §156 of the New York Penal Code (see 83 N.Y.2d 123, 629 N.E.2d 1034, 608 N.Y.S.2d 155 (1994)) and/or other applicable federal laws, and may be subject to criminal prosecution.