UNITED STATES DISTRICT COURT
for the
MIDDLE DISTRICT of PENNSYLVANIA

INTERNET POLICY

October 21, 1997
Revised September 20, 2001
Revised January 25, 2008

UNITED STATES COURTS
for the
MIDDLE DISTRICT OF PENNSYLVANIA

INTERNET POLICY

A. PURPOSE AND SCOPE

The United States District Court, United States Bankruptcy Court, and the United States Probation Office have adopted this policy for the authorized use of the Internet. These guidelines apply to all court employees and officers who are provided access to the court's computing resources for the conduct of official government business and to promote the mission of the court.

B. RESPONSIBILITY

Use of the Internet via computer gateways owned or operated on behalf of the United States Courts imposes certain responsibilities and obligations on court employees and officials and is subject to judiciary policies as well as local, state and federal laws. Court users must ensure that they use the Internet safely and productively and do not in any way compromise the interests of the judiciary. These guidelines apply to all Internet services and Intranet services, including but not limited to electronic mail, web browsers, Telnet and File Transfer Protocol (FTP). Acceptable use should always be ethical, reflect honesty and show restraint in the consumption of shared computer resources. It should demonstrate respect for intellectual property, ownership of information, system security mechanisms, and an individual's right to freedom from harassment and unwarranted annoyance.

Use of the Internet services provided by the court is subject to monitoring for security and/or network management purposes. Court users are therefore advised of this monitoring and consent to this practice. Monitoring includes the logging of all resources and "sites" which are accessed. Users should further be advised that many external Internet sites also log who accesses their resources, and may make the information available to third parties. By participating in the use of Internet systems provided by the court, users agree to abide by this policy as well as the court unit's official policies on computer use and security, limited personal use and network management. This policy hereby incorporates by reference the Code of Conduct for Judicial Employees which is applicable to all Internet activities. An employee's willful violation of the principles and provisions of this policy may result in disciplinary action.

C. PRIVACY AND SECURITY (see also Local Monitoring and Internet Blocking)

Access to the Internet is provided through the Judiciary's Data Communication Network (DCN). As part of the security system of the DCN's Internet gateway, a log is kept of all Internet activity passing through the DCN. The log is monitored at the gateway for improper use. If an individual accesses an Internet site or sends an electronic message through the DCN's Internet gateway, the fact that the activity originated from the United States Courts will be known by the receiving site or party. Inappropriate access can therefore be an embarrassment to the judiciary.

The Internet is not secure. Messages and information can be read or broadcast without the knowledge or consent of the author. Users should not expect that the messages they send or receive via the Internet will be private. Internet mail is also unreliable. Delivery and delivery times are not guaranteed due to unpredictable intermediary system and network outages, shutdowns, slowdowns and polling intervals. Users should not rely on Internet mail for time-sensitive communications or guaranteed delivery. Also, sometimes attachments to an email may not be readable by the receiving party. Note: The Lotus Notes "Receipt Requested" feature may not be honored by systems on the Internet. Users should not rely on this feature for Internet mail.

D. ACCEPTABLE USE

Court users of the Internet must adhere to the same code of ethics that governs all other aspects of Judiciary activity. The Internet may only be used for authorized activities and must be used in a professional, lawful and ethical manner in accordance with the restrictions contained herein. Limited personal use of the Internet may also be authorized by court officials subject to the restrictions set forth in paragraphs E, F and G, provided that such use is kept to a minimum and does not interfere with official business.

E. PROHIBITED USE

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

1. Sending data or files or mail over the Internet that contain any discriminatory statements that malign;

2. Making unauthorized commitments or promises of any kind that might be perceived as binding the government;

3. Sending confidential information over the Internet. The Internet is not a secure means of transmission and can cause confidential information to be compromised should it be read by an unauthorized party;

4. Taking part in Internet discussion forums that are not associated with official government business;

5. Posting opinions on the Internet to forums that are personal in nature;

6. Using the network connection for commercial or political purposes or for private gain;

7. Using the network for illegal activities such as illegal gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities;

8. Intentionally accessing sites or downloading or transmitting information that contains sexually explicit material, except when authorized as necessary to the employee's responsibilities.

F. ADDITIONAL PROHIBITED USES

Users may access only files and data that are their own, that are publicly available, or to which they have authorized access. Improper use or distribution of information is prohibited. This includes copyright violations such as software piracy. Users 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.

The use of peer-to-peer file sharing, chat rooms, and instant messaging for communicating with persons or entities outside the judiciary's private data communications network is prohibited. File sharing (using programs such as Napster, Grokster, Morpheus, and certain interactive Internet games), chat rooms, and outside instant messaging (such as AOL Instant Messenger) and Internet based telephonic programs such as Skype, are based on Internet technologies that circumvent the security protections provided by existing DCN.

G. ADDITIONAL INTERNET RESTRICTIONS

Users should refrain from any practices that might jeopardize the judiciary's computer systems and data files when downloading files from the Internet. Only material and software that is authorized and properly licensed may be downloaded, and files must be checked for viruses. Large downloads, such as those required by systems personnel in the performance of their duties, should be performed at non-peak times to avoid diminished network performance response time for other network users.

Caution should be exercised with regard to the volume and size of email being sent. Internet mailing lists can produce a high volume of messages automatically. In addition, attaching large files to email messages can drain the resources of the court's email system.

Access by judiciary personnel to personal Internet email accounts from within our networks is strongly discouraged. Use of these accounts poses threats to the judiciary's information technology infrastructure as most do not provide virus scanning of email and attachments.

> Judiciary personnel are reminded of the Judicial Conference policy, adopted at its September 2002 session, regarding Personal Use of Government Office Equipment (including Information Technology), which says that, unless further restricted by local court policy, judiciary employees are permitted limited use of government office equipment (including information technology) for personal needs if such use does not interfere with official business and involves minimal additional expense to the government. Sending and receiving a ***limited*** amount of personal email in your Lotus Notes court account is consistent with this personal use policy and far preferable to accessing a personal Internet email account from a computer security point of view.

Avoid the use of automatic email forwarding to personal Internet email accounts which can result in sensitive case or personal information being forwarded over network connections that are subject to interception by malicious outside Internet users. A safer alternative is to keep up with email while away from the office by using court-issued remote access via a virtual private network (VPN)

connection back to the court or to use a court-provided wireless email device (such as a Blackberry) to receive email, both of which provide secure email access to authorized off-DCN users.

Avoid advertising your email name over the Internet. In particular, limit the recipients of your email messages to people and organizations you know. Do not arbitrarily hit "Reply All" to messages with mail lists or people you do not know. This helps reduce the possibility that your personal or court email name will be captured by spammers, phishers, or other malicious Internet users.

H. LOCAL MONITORING AND INTERNET BLOCKING

To ensure a baseline network management policy and to assist with providing a level of compliance with the acceptable use policy for court users of the Internet, the district will implement software such as WebSense, SNORT, Wire Shark, Sniffer, Etheral and other tools that may be available for blocking and monitoring at the local level.

1. Personal Web Based email accounts will be blocked except those identified by the Administrative Office which provide virus scanning of email and attachments such as AOL's AIM Mail, Google's Gmail, MSN Hotmail and Yahoo Mail. Any exceptions to this policy must be reviewed by the A.O. and approved by the Chief Judge.

2. To avoid decreases in network capacity and to minimize system downtime which can occur due to the use of bandwidth-intensive applications such as streaming media or Internet Radio, the following internet protocol activity will be blocked between 8:30 AM and 5:00 PM, Monday through Friday:

- Internet Radio and TV
- Streaming Media (Audio/Video)

3. The following site categories will ***always*** be blocked unless otherwise approved:

- Adult/Sexually Explicit
- Chat Rooms and Instant Message
- Gambling
- Hacking
- Intolerance and Hate
- Illegal Drugs
- Peer-to-Peer file sharing networks
- Phishing & Fraud (identity theft)
- Spyware (live viruses)
- Tasteless & Offensive
- Violence

Judiciary employees may have a business purpose in accessing a blocked site, or an appropriate site may be blocked for some unknown reason. If this is the case, access rights may be restored, upon

email request, following the approval of the appointing judge or unit executive. Such request must indicate the specific site that is blocked and the reason access is needed. Once approved, the email shall be forwarded to the systems manager of the court unit for appropriate action.

H. ENFORCEMENT OF POLICY

An investigation may be conducted if the appointing judge or unit executive suspects that an employee has committed a violation of this policy. During an investigation, the employee is notified and given an opportunity to provide an appropriate justification. If the appointing judge or unit executive does not find the explanation to be adequate and believes that an abuse of Internet privileges and computer use may have occurred, the appointing judge or unit executive may authorize the systems manager to produce a report of that employee's Internet activity.

Such report shall be limited only to the Internet and computer use activities of the employee in question. Thereafter, the report may be used as the basis for disciplinary action. Any report produced shall be confidential and viewed only by those individuals designated by the judge or unit executive.

Any employee who violates this policy will be subject to the full range of disciplinary actions, including termination.

This policy may be amended at any time by the Board of Judges.

Adopted by the Board of Judges on January 25, 2008.

For the court,

s/ Yvette Kane
Yvette Kane
Chief, U.S. District Judge

CERTIFICATION

I have read and understood this policy.

_____ _____
Employee's Signature Date

United States District Court, Middle District of Pennsylvania

Social Network Computer Policy (November, 2009)

The birth and advance of "Web 2.0" technologies and applications in recent years has the potential to revolutionize how individuals, corporations, government agencies, and non-profit organizations interact and communicate with one another. Web 2.0 refers to the second generation of web design and software development, which places heavy emphasis on communication, collaboration, and sharing among internet users. Unlike the first generation of internet (Web 1.0), this change is grounded less in major technical transformations. Instead, this change is centered, chiefly, on the ways individuals use the Internet. Before Web 2.0, most Internet users were mainly consumers of information; now, these new technologies and applications allow users to be both producers and consumers of information and shift easily between those roles.

Many of these Web 2.0 applications, often called "social media," are central parts of many people's daily computer usage. Users, whether they be institutions or individuals, connect and communicate through social networking internet sites; collaborate on, refine, and disseminate knowledge through wikis; share their perspective through blogs and microblogs; upload still and video images through videosharing and photosharing sites; broadcast via podcasts and vodcasts; and stay connected via RSS feeds beamed to e-mail inboxes or displayed on smartphones.

As Web 2.0 has made communication instantaneous and allowed for greater collaboration and information sharing, there has been some downside. Many users adopting Web 2.0 seem less concerned, or at least mindful, of privacy and confidentiality as they navigate social media sites such as Facebook. Recent news stories illustrate the privacy and confidentiality concerns generated by the expansion of social media internet usage: employment opportunities lost because of Facebook profiles; scandal precipitated by YouTube or Flickr postings, and judicial proceedings compromised by jurors' Twitter postings.

The challenges and risks of this social media environment, though, are particularly acute for government employees that work in positions where discretion and confidentiality are imperative. Court employees work in such an environment. Court personnel are expected to keep sensitive information confidential, exercise discretion to avoid embarrassment to the Court, and take precautions to avoid unnecessary security risks for court personnel, especially the judges they serve.

The Court has set down a series of broad guidelines for employees to consider as they navigate these new, and ever changing, technologies and applications.

1. **Think before you post**. Internet postings – whether they be text, photos, videos, or audio – remain accessible long after they are forgotten by the user. Beyond that, remember that nothing is "private" on the Internet despite people's best efforts to keep things private. Do not post anything on the Internet that you would not want to read on the front page of the local or national newspaper.