UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CLERK'S OFFICE EMPLOYEE

INTERNET ACCESS AGREEMENT

General Provisions

In compliance with Judicial Conference Policy regarding Internet access for computers connected to the Data Communications Network (DCN), the following general and specific provisions apply to all clerk's office employees of the Central District of California:

1. Use of the public Internet network accessed via computer gateways owned or operated on the behalf of the United States District Court for the Central District of California ("the Court"), imposes certain responsibilities and obligations on Court employees and officials ("Users"), and is subject to Court policies and local, state and federal laws. Acceptable use is ethical, reflects honesty, and shows restraint in the consumption of shared computing resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and an individual's right to freedom from harassment and unwarranted annoyance.

2. Use of the Internet services provided by the Court is subject to monitoring. Users of these services are therefore advised of this monitoring and agree to this practice. This monitoring may include a review of internet e-mail messages sent and received, and which Internet resources and sites are accessed. Users should further be advised that many external Internet sites also log who accesses their resources, and may make this information available to third parties.

3. By participating in the use of the Internet systems provided by the Court, Users agree to be subject to and abide by this Policy for their use. Willful violation of the general or specific provisions of the Policy may result in disciplinary action, including termination.

Specific Provisions

1. Users will not utilize the Internet network for illegal, unlawful, or unethical purposes or to support or assist such purposes. Examples of this would be the transmission (including uploading or downloading files) or viewing of violent, threatening, defrauding, obscene, or unlawful materials. Creating, downloading, viewing, storing, copying, and transmitting sexually-explicit or sexually-oriented materials is never appropriate and may be illegal in some cases.

2. Users will not utilize the Internet network equipment for partisan political purposes or commercial gain.

3. Unless for official business, judiciary employees should not use the network connection for commercial purposes (including shopping). It is also inappropriate to use the network connection in support of outside employment activities (including consulting for pay, sales or administration of business transactions, and sales of goods or services) or for illegal activities (such as gambling or hacking).

4. Users will not utilize the Internet systems or messaging services to harass, intimidate or otherwise annoy other persons.

5. It is not appropriate to use government systems to send or receive e-mails containing greeting cards, political statements, jokes, pictures, sexually-explicit or sexually-oriented materials and other items of a personal nature. Chain letters or other unauthorized mass mailings, regardless of the subject matter, likewise are inappropriate. Checking personal web e-mail accounts from the Court's private data communications network raises severe security risks locally and judiciary-wide and is prohibited.

6. Users will not utilize the Internet to disrupt other users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses, and

sustained high volume network traffic which substantially hinders others in their use of the network. Logging onto video or audio sites, such as broadcast services or radio stations, degrades the performance of the entire network and is prohibited. Downloading music files consumes significant disk space on local computers and may be a violation of copyright law.

7. Users will only utilize the Internet network to access files and data that are their own, that are publicly available, or to which they have authorized access.

8. Because files or matters obtained over the Internet may contain destructive computer viruses that may be harmful to the Court's network, downloading attachments to e-mail or files obtained via the Internet (as opposed from the Intranet or DCN) shall be strictly limited to either: (1) items expressly requested by the Users from known senders, or (2) unrequested files transmitted to Users by known senders. Users shall not download and open any attachments to files, or open any e-mail, that is received or made available to the Users from an unknown Internet source.

9. Users will not remove Court scanning software. If the software is removed or not activated and use of the Internet has been or is being performed, the Users may lose their right to access the Internet and the DCN.

10. Users will refrain from monopolizing systems, overloading networks with excessive data, or otherwise disrupting the network systems for use by others. Video, sound or other large file attachments consume large amounts of network capacity. E-mail attachments, large files, and executable programs present two problems: first, large attachments consume network capacity and storage space on both national and local e-mail servers and desktops, slowing the network down for everyone; and second, executable programs

present a risk for infection by computer viruses.

11. Judiciary employees should only participate in chat rooms when directly relevant to their official duties and responsibilities. All other non-business related chat rooms are prohibited. When participating in a chat room, employees should not inadvertently give the impression of articulating official judiciary policy or positions. 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.

12. It is not appropriate to use e-mail or the Internet to access, send or receive information on or in support of activities that are illegal or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

13. Blogging in support of activities that are illegal, offensive or disparaging to fellow employees, the public or the judiciary, or that gives the impression of pronouncing official judicial policy, is prohibited.

By signing this Agreement, I agree to abide by the general and specific provisions outlined and understand that use of the public Internet is a privilege that can be revoked if improperly used.

Dated	*Employee Signature*
	Print Name
	Department