

Board of Judicial Policy and Administration
Policy Statement for the Use of Computers, Electronic Mail, and Internet
Replacing Policy Issued September 10, 2001

The policy of the Board of Judicial Policy and Administration for the use of computers, Internet, and electronic mail is designed to guide effective and appropriate use of those resources. The policy applies to judicial branch employees who are a user or subscriber of Internet access or other electronic resources through the Judicial Network administered by the Wyoming Supreme Court Technology Office. The use of computers, Internet, and electronic mail is encouraged in order to fulfill the following requirements:

1. Further the operations of the Judiciary.
2. Provide effective and responsive service to the public.
3. All electronic resources, including the Internet, are provided for court business. Electronic communications and use of the Internet for activities relevant to an employee's personal life or family are permitted to the extent they do not distract from the dignity of the judiciary or interfere with the performance of the employee's normal work duties or equipment.
4. Internet access is offered as a courtesy, and is therefore subject to the local usage discretion of each judge or supervisor concerning their specific staff or location and restrictions which go beyond this policy.
5. All electronic communications with, and content stored on, court equipment is not to be considered private or personal to any individual employee, contractor, volunteer, or third party.
6. Data on the Supreme Court's network will be protected from unlawful disclosure. It is important for each user, however, to understand that all information on the Judicial Network housed in the Supreme Court and on court computer assets belong to the Judicial Branch.
7. Authorized users shall not allow or facilitate another employee, contractor, volunteer, or the public to access internal court resources using their authorized account or personally assigned credentials, such as a username or password. This includes email, case management, data warehouse (SCIS) resources, etc.
8. No user shall intentionally or negligently damage or interfere with the operation of, or prohibit authorized access to, court information or other technology-related resources.
9. No user shall store or distribute copyrighted material utilizing state owned assets or networks.
10. The Court Technology Office (CTO) may periodically audit, inspect, and monitor any user's network activity, and all data stored on state issued equipment. This includes, but is not limited to monitoring sites visited by employees on the Internet, chat groups, newsgroups, blogs, and reviewing material downloaded from or uploaded to the Internet from personal equipment. In addition, the CTO may limit or block access to specific online resources not required for conducting court business, such as streaming audio or video. Monitoring, auditing, or investigating specific employee access to, or use of electronic resources by the technology office must be explicitly requested and approved by a local judge or supervisor. If evidence of abuse is identified by the CTO, it shall be furnished to the Court Administrator.

Inappropriate Conduct or use of Internet and Electronic Mail

Any of the following activities will be considered a violation of this policy:

1. Use of Internet or electronic mail that violates federal or state laws.
2. Use of Internet or electronic mail to transmit or obtain threatening, obscene, harassing, or malicious materials.
3. Use of abusive or objectionable language either in public or private messages.
4. Misrepresentation of oneself or the Judicial Branch.
5. Activities or uses that may cause congestion or disruption of networks or systems, including but not limited to such activities as the distribution of chain letters for unsolicited advertising.
6. Using the court's electronic services for the downloading of personal software, screensavers, or third party software that puts any court resource or information at risk or system malfunction.
7. Downloading, copying, distributing, or storing movies, music, software, books, etc. in violation of copyright laws.
8. Using the court's resources for viewing or distributing content which is considered violent, offensive, graphic, or sexually explicit.
9. Using the court's resources to post or transmit any message or material which is libelous, defamatory, or which discloses private, confidential, or personal matters concerning any person, case, or group.
10. Using the court Internet for running a private business, operating a personal web site, or actions to avoid or side-step violations of this policy.
11. Usage of court provided Internet to participate in partisan political activities.

Exceptions

Requests for exceptions to this policy must be submitted to the CTO in writing for review. The request must specifically state the scope of the exception along with justification for granting the exception, potential impact, or risk. The CTO will review requests, confer with the requesting judge, and Court Administrator if necessary.

Violation of this policy constitutes grounds for sanctions by the Board of Judicial Policy and Administration and subjects the employee to appropriate disciplinary action. Non-employees who violate this policy may be subject to termination of contractual agreement, denial of access, and any other applicable penalties.

Dated this 6th day of January, 2011.

Board of Judicial Policy and Administration



By: _____
Chief Justice Marilyn S. Kite