Minnesota Judicial Branch Policy

Policy Source:	Judicial Council
Policy Number:	317
Category:	Human Resources
Title:	Use of the Internet and Other Electronic Communication Tools
Effective Date:	October 1998; April 21, 2006; December 14, 2006; March 15, 2007; December 15, 2009; April 1, 2012; May 15, 2016; January 1, 2021; December 1, 2022, September 1, 2023
Revision Date(s):	April 21, 2006; December 14, 2006; March 15, 2007; December 15, 2009; April 1, 2012; March 17, 2016; November 19, 2020; October 20, 2022, August 17, 2023
Supersedes:	

Use of the Internet and Other Electronic Communication Tools

I. POLICY STATEMENT

The Minnesota Judicial Branch provides a variety of electronic tools such as telephones, cellular phones, computers, mobile computing devices, facsimile machines, electronic mail (e-mail) systems, Lync, and internet access, for employees and judges whose job performance would be enhanced by the technology. The Judicial Branch faces the challenge of making maximum use of the benefits of such tools, meeting legal requirements for access to information, and providing adequate protection for proprietary information. This policy governs access to and the appropriate use of this technology during work times as well as time periods before and after work and during break periods by Judicial Branch employees and judges. This policy shall also govern access to and appropriate use of court technology by any contractor paid in whole or in part from court funds or individual serving voluntarily without pay or other form of compensation.

A. Judge and Employee Responsibility

Judicial Branch judges, employees, volunteers, and independent contractors are responsible for appropriate use of the internet and other electronic communication tools in accordance with this policy. They are expected to adhere to the highest ethical standards when using the internet and other electronic communication tools.

Employees and judges are prohibited from using a password or ID assigned to another employee or judge without the employee's or judge's permission. Employees and Judges are prohibited from sharing system passwords and IDs under this policy unless the sharing of system passwords and IDs is necessary and no alternative to shared passwords exists.

Nonexempt employees are not permitted to monitor or respond to work related emails or other electronic communication outside of normal working hours unless they have been specifically directed to do so by their supervisor and are being compensated for their time or the time spent on the activity is de minimis[1].

B. Management Responsibility

Managers and supervisors are responsible for ensuring the appropriate use of all electronic communication tools, including e-mail and internet access, through training, supervising, coaching, and taking disciplinary action, when necessary.

Nonexempt employees shall not be assigned or directed to monitor and respond to work related emails or other forms of work-related electronic messaging outside of normal working hours unless they are being compensated for the activity or the time spent on the activity is de minimis.

C. Appropriate Use

The internet and other electronic communication tools are to be used for business purposes that increase timely and effective business communications of the Judicial Branch. Limited and reasonable use of Judicial Branch time, property, or equipment (including internet and other electronic communication tools) to communicate electronically for private purposes, is permitted, provided this use, including the value of the time spent:

- Results in no cost to the Judicial Branch or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impracticable. (Source: M.S. §43A.38, subd. 4);
- Does not interfere with business usage;
- Does not interfere with the employee's and judge's job activities;
- Does not interfere with other employee's and judge's job activities; and
- Does not otherwise violate this or any other Judicial Branch Policy (including, without limitation, Judicial Council Policy 318; Employee Code of Ethics; Judicial Council Policy 306, Outside Employment; and Judicial Council Policy 317, Electronic Communication, section I.D. Inappropriate Use, below).

D. Inappropriate Use

Uses of the internet and other electronic communication tools that will not be tolerated include, but are not limited to:

[1] "De Minimis" means insubstantial or insignificant amounts of time beyond a worker's scheduled hours; the amount of time involved must be so small, indefinite, or uncertain that the employer cannot, as a practical matter, record the time.

- Illegal activities;
- Wagering, betting, or selling;
- Transmission of harassing, disparaging, intimidating, abusive or offensive material to or about others;
- Commercial activities, e.g., personal for-profit business activities;
- Solicitation, except on agency-sanctioned activities;
- Promotion of political or private causes, positions or activities, and/or other unethical activities;
- Activities that demean the dignity of the court;
- Transmission, receipt, storage, display or viewing of, material that is or may be reasonably regarded as violent, harassing, discriminatory, obscene, sexually oriented or pornographic, including any depiction, photograph, audio recording or written word;
- Unauthorized access or use of public and non-public data;
- Non-Judicial Branch judge or employee use (e.g., family member or friend) at work or away from work;
- Uses that are in any way disruptive or harmful to the reputation or business of the Judicial Branch;
- Purposes other than Judicial Branch business, except limited and reasonable personal use;
- Sharing of system passwords and IDs unless sharing of passwords and ID²s is necessary and no alternatives exist;
- Using a password or ID assigned to another employee or judge without the employee's or judge's permission.

Review of material which would otherwise be prohibited under this policy is permitted for case related or other business-related review purposes.

E. Storage, Retention and Disposition

The State Court Administrator's Office will provide specific guidance on storage, retention, and disposition of electronic messages.

F. Utilization of Courts' Email Address

Because each internet e-mail user's identification includes the suffix @courts.state.mn.us, it is imperative that judges, employees, volunteers, and independent contractors shall refrain from using the courts' email address in news groups, chat groups, online shopping, bulletin boards, or anything else where the content is not clearly work-related because such messages might be construed as an official State of Minnesota or Judicial Branch position.

G. Social Media and Court Business:

The Court Employee Code of Ethics prohibits employees from engaging in communication regarding cases before the court unless necessary to discharge their

official duties; this prohibition includes using social media to comment on cases or business before the court.

H. Proper Internet Use

Internet and e-mail use must be able to withstand public scrutiny without embarrassment to the Judicial Branch, its customers, its judges, or its employees, if messages are forwarded beyond the intended recipients, accessed or inadvertently disclosed, subpoenaed in a legal action, or otherwise made public. Judges, employees, volunteers, and independent contractors should use generally accepted standards of business conversation in all internet and e-mail communications and use good judgment in the type of message created, tone, and content of messages. Content is always considered personal opinion unless specifically set forth as a Judicial Branch or specific court position.

The use of Large Language Model Artificial Intelligence (e.g. ChatGPT) is restricted, as use of these tools pose unique risks for the Branch which require significant caution and discretion. Judges, employees, volunteers and independent contractors with a business reason for use must submit an IT service request for approval by the Cyber Security Unit. Access may be revoked at any time.

I. Monitoring

Electronic communication devices such as telephone, Judicial Branch provided cellular phones, facsimile machines, mobile computing devices, Judicial Branch e-mail systems, and internet access are Judicial Branch property. Like other Judicial Branch resources, they are intended to be used for Judicial Branch business and other agency-sanctioned activities. The Judicial Branch reserves the right to monitor all use of Judicial Branch provided cellular telephones, telephones[2], facsimile machines, pagers, mobile computing devices, e-mail, and internet resources. Any and all software, data or other information stored on a Judicial Branch-owned computer may be monitored, read, examined, seized or confiscated as necessary at the time of use, during routine post-use audits, and during investigations. Therefore, employees and judges should not expect that any facsimile, voicemail, or e-mail message either sent or received, or any internet activities will remain private. (Similarly other Judicial Branch-owned property, including but not limited to locked/unlocked desk drawers and cabinets, vehicles, and equipment may also be seized, confiscated, and or searched as necessary.) Judges and employees should not expect that any personal property that is maintained and/or stored in Judicial Branch work sites would remain private. The Judicial Branch reserves the right to monitor any use of these systems, including use of these systems while the employee or judge is on their own time, to access any information on these systems, and to take any action it determines to be appropriate with respect to that information.

[2] Electronic monitoring of telephone conversations will only occur if proper notice has been given, in accordance with Federal regulations for Stored Wire and Electronic Communications and Transactional Records Access (Federal Wire Tap Regulations) See 21 U.S.C. 2701-2711.

It is a supervisory responsibility to oversee use and to determine if internet and other electronic communication tools are appropriate to assigned work. Content of e-mail messages is not routinely monitored or disclosed. However, judges, employees, volunteers, and independent contractors should understand that e-mail messages and internet transactions, including those they delete or erase from their own files, may be backed up or recorded and stored centrally for system security and investigative purposes. They may be retrieved and viewed by someone else with proper authority at a later date. Monitoring or disclosure may occur internally under administrative procedure and externally under subpoena or other legal actions, in connection with charges of improper or illegal actions by an individual, unexpected absence of an employee or judge, or upon request for public data and other appropriate business or technical reasons.

J. Downloading of Software

Unless authorized by the appointing authority, judges, employees, volunteers, and independent contractors shall not download software residing on the internet. Downloading presents a significant risk of virus infection and license fee liability, and some of the software residing on the internet is inherently unreliable. If downloading is appropriately authorized, employees and judges must follow designated procedures for file transfer, virus scanning, and licensing. Judges and employees should not assume that software is available for public use free of charge simply because there in no copyright or other intellectual property notice in or on the software. U.S. copyright law, and that of many other countries, no longer require a copyright notice as a prerequisite to copyright protection.

K. Anti-Virus Measures

Incoming e-mail messages containing attachments may imperil Judicial Branch systems by importing viruses. Such attachments should be routinely scanned for viruses prior to using or executing the attachments.

L. Software Piracy Policy

Any software introduced by a judge, employee, volunteer or independent contractor into the workplace must be licensed and used in accordance with the license. It is the responsibility of the judge, employee, volunteer or independent contractor introducing such software to produce the license upon demand or be subject to discipline and/or be responsible for indemnifying the Judicial Branch for any liability incurred by it.

II. IMPLEMENTATION AUTHORITY

Implementation of this policy shall be the responsibility of the chief judges of the ten judicial districts and the Court of Appeals, the Chief Justice of the Supreme Court, and the State Court Administrator.

Implementation of this policy with respect to payment for telephones, facsimiles and portable electronic devices shall be the responsibility of the State Court Administrator or designee, acting as the agent of the Judicial Council.

III. RELATED DOCUMENTS

- *Minnesota Judicial Branch Policy 205(f) Payment and Cyber Security Requirements for Telephones, Cell Phones, Smart Phones, Mobile Devices, and Legacy Arrangements for Home Internet*
    - *Minnesota Judicial Branch Procedure 205(f) Appendix A: Charges for Personal Calls or Data Usage*
    - *Minnesota Judicial Branch Procedure 205(f) Appendix B: Cell Phone, Smart Phone, Mobile Device, and Home Internet Connectivity Allowance Form*
    - *Minnesota Judicial Branch Procedure 205(f) Appendix C: Phone, Mobile Device, and Home Internet Connectivity Allowance Rate Schedule*
- *Minnesota Judicial Council Policy 318 Court Employee Code of Ethics*