ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 5: Automation
Section 1-503: Electronic Communications

A. Definitions. In this section, unless otherwise specified, the following definitions apply.

"Appointing Authority" means the judge, clerk of court, administrator, or their designee who is designated to supervise authorized users.

"Court" means all Arizona judicial department courts and offices subject to this policy.

"Electronic communication" means, but is not limited to, electronic mail ("email"), accessing the Internet ~~services~~, voice-mail, text messages, chat messages, video content, and facsimile messages that are sent or received by judicial officers and employees, and other authorized users, and the network resources over which such communications are transmitted.

"Internet" means the global network connecting millions of computers and includes, but is not limited to, access to the World Wide Web.

"Official communication" means a communication pertaining to public business, which must be preserved as a record of official action or policy.

"Users" means all court officials and employees who have access to the Arizona Judicial Information Network (AJIN) ~~and also~~ as well as any non-court persons who are authorized users.

"Work-related, Internet-accessible resources" means, but is not limited to, software applications, resources, and storage locations that reside outside of AJIN or an individual court network that are necessary for accomplishing the job duties of a court employee, contractor, or volunteer.

B. Purpose.

1. Electronic communications and Internet technology allow access to a broad range of ideas and information~~,~~ and facilitate the exchange of ideas and information in a timely and efficient manner. The judicial department supports the use of electronic communications, networked information, and Internet resources to further its mission and to foster communication and information exchange within the court and the justice community. The purpose of this section is to set forth the guidelines and mutual responsibilities for managing and using the Arizona Judicial Information Network (AJIN) electronic communications resources, ~~and~~ Internet access, and work-related, Internet-accessible resources. The Administrative Office of the Courts (AOC) is responsible for operating and managing AJIN, electronic communications resources and Internet access, and for ensuring that AJIN's resources are used to support the business of the local court and the judicial department through implementation of appropriate policies and procedures. AJIN users are expected to be cognizant of the rules and conventions that make these resources secure and efficient, and

to use the resources in a responsible manner, consistent with the work-related, professional, and educational purposes for which these resources are provided.

2. Persons Covered. The section applies to all courts using AJIN and work-related, Internet-accessible resources and the users of those resources. Courts not using AJIN for their electronic ~~mail~~ communications or Internet access are required to have substantially similar written electronic communications policies.

3. Authorized Use. Users ~~shall~~ must use electronic communications resources and Internet access responsibly for court purposes relating to the business of the court ~~or enhancing the work environment of the court~~, as set forth in this section. ~~Those~~ AJIN users ~~who~~ are not permitted to connect ~~bring~~ their own personal ~~computers~~ devices to ~~work~~ AJIN ~~and~~ but may access ~~the Internet~~ work-related, Internet-accessible resources from personal devices ~~those computers, as well as those who access email and the Internet from remote locations via any dial-up connection through AJIN, are also subject to this section~~.

4. Relationship to Other Rules. Use of computers, electronic communications and Internet resources is subject to all other rules governing the judicial department and court personnel, including the code of conduct, equal employment opportunity~~,~~ and ~~or~~ sexual harassment policies and Rule 123, ~~Rules of the Supreme Court of Arizona~~, ~~governing~~ which governs public access to court records. All users must complete the annual computer security/network training, required under ACJA §1-302, to ensure working knowledge of current measures strengthening the security of the Arizona judiciary's data, systems, and network to protect confidentiality, integrity, and availability of information. Each local court's policies and procedures must be at least as stringent as this section, may further clarify this section, or ~~provide for~~ include more restrictive computer/network security access and awareness provisions ~~of these policies~~ for its staff. Statements in this section regarding permissible and prohibited uses of electronic communications, ~~and~~ the Internet, and work-related, Internet-accessible resources are intended as ~~additional~~ guidelines and examples.

C. Responsible Use of Electronic Communication and Internet Resources.

1. Responsible Use of Electronic Communications.

   a. Professionalism. Electronic communications ~~shall~~ must be professional and ~~business-like~~ business-appropriate. Electronic ~~mail messages~~ communications, whether sent within the judicial department or outside the judicial department via wide area networks or the Internet, must withstand public scrutiny without embarrassment to the local court, the judicial department, other users, and the public, both as received by the original recipient and if forwarded beyond the original intended recipient.

   b. Professional Use. ~~It is permissible to use t~~The judicial department's ~~email~~ electronic communication systems may be used for ~~limited~~ professional purposes. ~~Approved~~ Examples of professional uses include:

(1) Participation in professional associations;
(2) Continuing education;
(3) Scholarly publication;
(4) Communications with colleagues; and
(5) Subscription to listservers, news ~~groups~~ feeds, or topical updating services related to the local court, the judicial department, or a user's professional duties. Users subscribing to these services ~~shall~~must:
    (a) Keep up with the ~~mail~~ communications received, regularly deleting messages once read;
    (b) Learn the rules associated with the service;
    (c) Know how to unsubscribe (both for ending participation and during absences or vacations)~~,~~; and
    (d) Maintain a professional demeanor when posting to a list.

~~This~~ Notwithstanding the above examples, any professional use is subject to ~~approval~~ disapproval ~~of~~ by the user's appointing authority.

c. Routine Use. The judicial department's communication systems may be used for routine business and personal purposes.

(1) Routine Business Use. ~~Routine~~ Examples of routine business use ~~is permissible and includes~~ include:
    (a) Scheduling and attending work-related meetings;
    (b) Requesting work-related information;
    (c) Assigning of work tasks;
    (d) Clarifying of work assignments;
    (e) Notifying others of a user's whereabouts~~,~~; and
    (f) ~~Making~~ Requesting sick, ~~days or~~ vacation, or other leave ~~requests~~.
(2) Routine Personal Use. ~~Routine~~ Examples of routine personal use ~~is permissible and includes~~ include:
    (a) Notifying family members of schedule changes;
    (b) Sending appropriate personal messages to co-workers~~,~~; and
    (c) Communicating information that is typically permitted in or from the workplace in person or by ~~telephone~~ another medium.

Routine personal use of electronic communications is not permissible ~~does not include~~ if it involves expending substantial work~~place~~ time or resources, ~~using email~~ for personal, charitable, or ~~partisan~~ political solicitations or campaigns, or ~~using email~~ for purposes that would otherwise violate court policies with regard to a user's time commitments or court equipment. It is the responsibility of the user sending ~~these~~ personal messages to ensure that the message is identified, either ~~specifically~~ expressly or clearly understood by its content, as personal in nature~~,~~ and not on behalf of the court. Notwithstanding the above examples of routine personal use, any ~~Routine~~ routine personal use is subject to ~~approval~~ disapproval ~~of~~ by the user's appointing authority.

d. Official Use. A user ~~may transmit~~ electronically transmitting or receiving official communications ~~via email as long as they are created~~ must create and ~~preserved~~ preserve them in compliance with applicable record retention and destruction schedules.

2. Prohibited Uses of Electronic Communications.

a. Commercial Purposes. Users ~~shall~~ must not use electronic communications for commercial purposes.

b. Malicious Purposes. Users must not send or forward a "serial" or "chain" message, spam e-mail, or phishing message, or intentionally violate approved cybersecurity policies. Only authorized individuals may be allowed to distribute periodic phishing tests, in coordination with AJIN management, to improve employees' security awareness levels.

~~b.~~c. Copyright and Intellectual Property Rights. Users ~~shall~~ must not use electronic communications to receive or send copies of documents in violation of copyright laws, or to send or receive software in violation of intellectual property laws or rights.

~~c.~~d. Harassment. Users ~~shall~~ must not use electronic communications to intimidate or harass others~~,~~ or to interfere with the ability of others to conduct court business. Users ~~shall~~ must not use electronic communications in a manner that promotes, constitutes, or could reasonably be interpreted as promoting or constituting discrimination on the basis of race, creed, color, gender, religion, disability, age, or sexual preference.

~~d.~~e. Identification. Users ~~shall~~ must clearly identify themselves in any electronic communication, and ~~shall~~ must not construct an electronic message or communication ~~which~~ that appears to be from anyone other than the user (~~"~~spoofing"). Shared mailboxes must clearly identify the court and department on behalf of which the communications are made.

~~e.~~f. Unauthorized Access. Users ~~shall~~ must not capture and "open" electronic communications addressed to others, except as required for authorized staff to diagnose and correct delivery problems, and ~~shall~~ must not obtain access to the files or communications of others unless doing so serves a legitimate business purpose.

~~f.~~g. Privacy. AJIN users have no expectation of privacy. Even though users routinely use ~~email as a form of communication~~ electronic communications to discuss ideas and pending ~~cases~~ matters, they should not consider this form of communication as secure nor any message as absolutely confidential. Electronic mail, particularly when sent via the Internet, is an unsecured medium. More information about electronic mail (including copies of the content of messages) is routinely recorded than may be recorded using other communications media. A broader, less controlled set of people may have or gain access to electronic mail, and messages ~~are too easily~~ may be delivered or forwarded in error.

~~g.~~h. Confidential Communications. The confidential or privileged status of a communication is determined by court rule, order, or statute, and may include communications relating to employee performance or discipline, and judicial or attorney work product. It is the user's responsibility to carefully consider the confidentiality requirements of an electronic communication before it is transmitted.

~~h.~~i. Software. Users ~~may~~ must not use AJIN to download software, unless they comply with established AJIN policies for obtaining approval for loading or operating software on court provided computers, verifying proper licensing, and scanning for computer ~~viruses~~ malware.

~~i.~~j. Adherence to Security Restrictions on Systems and Data. Users ~~shall~~ must not attempt to gain unauthorized access to data, to breach or evade any security measures on any electronic communication system, or to intercept any electronic communication transmissions without proper authorization and a documented reason to do so.

3. Responsible Use of the Internet.

a. Professionalism. Use of the Internet ~~shall~~ must be professional and ~~business-like~~ business-appropriate. Any use ~~shall~~ must withstand public scrutiny without embarrassment to the local court, the judicial department, other users, and the public.

b. Professional Use. ~~Users may use~~ AJIN's Internet access may be used for ~~limited~~ professional purposes ~~with the approval of the appointing authority~~. ~~Approved~~ Examples of professional uses include:

(1) Participating in professional associations;
(2) Obtaining continuing education;
(3) Accessing or publishing scholarly publications~~,~~; and
(4) Performing legal research related to the local court, the judicial department, or a user's professional duties.

~~This~~ Notwithstanding the above examples, any professional use is subject to ~~approval~~ disapproval ~~of~~ by the user's appointing authority.

c. Routine Use. AJIN's Internet access may be used for routine business and personal purposes.

(1) Routine Business Use. ~~Routine~~ Examples of routine business use ~~is permissible and includes, but is not limited to~~ include:
(a) Locating information on a particular topic for ~~work~~ work-related use;
(b) Accessing other courts' information and sites; and
(c) Accessing information ~~by~~ of various professional organizations.

(2) Routine Personal Use. ~~Routine~~ Examples of routine personal use ~~is permissible and includes~~ include using the Internet for locating information relating to personal interests. Routine personal use ~~does~~ of the Internet is not ~~include~~ permissible if it involves:

(a) Expending substantial ~~workplace~~ work time, computing resources, or network resources;

(b) ~~Using a~~Access for personal, charitable, or ~~partisan~~ political solicitations or campaigns~~,~~; or

(c) ~~Using a~~Access for purposes that would otherwise violate court policies with regard to a user's time commitments or court equipment.

~~It~~ The user is ~~the responsibility~~ responsible ~~of the user using the Internet to ensure~~ for ensuring that the use complies with all current policies. ~~This use is, in all respects,~~ Notwithstanding the above examples, any routine personal use is subject to ~~approval~~ disapproval ~~of~~ by the user's appointing authority.

d. User~~'s~~-Owned Personal ~~Computer~~ Devices. ~~Those users~~ Users who ~~bring their own personal computers to work and access the Internet from those computers, as well as those who access email and the Internet from remote locations via any dial-up connection through AJIN,~~ access work-related resources on the Internet using personal devices ~~shall~~ are also ~~be~~ subject to the ~~requirements in~~ provisions of this section.

e. Public Use of Wireless Internet within Buildings. Public users will not be granted access to the AJIN wireless network without first expressly agreeing to abide by usage guidelines summarizing the key requirements of this section applicable to the public. Before login is permitted, public users will be required to review and accept these usage guidelines.

4. Prohibited Uses.

a. Commercial Purposes. Users ~~shall~~ must not use the Internet or AJIN for any commercial purpose ~~purposes~~. For purposes of this Section, "commercial purpose" means any purpose in which the user can reasonably anticipate the receipt of monetary gain from direct or indirect use of the Internet or AJIN.

b. Malicious Purposes. Users must not intentionally create or distribute malicious messages, attachments, spam emails, phishing messages, or malware. Only authorized individuals may be allowed to distribute periodic phishing tests, in coordination with AJIN management, to improve employees' security awareness level.

~~b.~~c. Copyright and Intellectual Property Rights Violations. Users ~~shall~~ must not use the Internet resources provided by AJIN in violation of copyright laws, or to download or receive software in violation of intellectual property laws or rights.

~~c.~~d. Harassment. Users ~~shall~~ must not use the Internet access provided by AJIN to intimidate or harass others; ~~or~~ to interfere with the ability of others to conduct court business; ~~Users shall not use the Internet access provided by AJIN~~or in a manner that promotes or constitutes, or could reasonably be interpreted as promoting or constituting, discrimination on the basis of race, creed, color, gender, religion, disability, age, or sexual preference.

~~d.~~e. Other Prohibited Uses. Users ~~shall~~ must not use the Internet access provided by AJIN for connecting to, posting, downloading, or printing pornographic, offensive, or other material that is inappropriate for the workplace ("NSFW") or violates the code of conduct, equal employment opportunity, sexual harassment policies, or A.R.S. § 38-448.

~~e.~~f. Software Downloading. Users ~~shall~~ must not use the Internet access provided by AJIN to download software, unless they comply with established policies for approval of loading or operating software on court provided computers, verification of proper licensing, and scanning for computer ~~viruses~~ malware.

~~f.~~g. Unauthorized Access. Users ~~shall~~ must not obtain access to the files or communications of others for any purpose unless doing so serves a legitimate business purpose, as approved in writing by an appointing authority.

~~g.~~h. Violations of Security Restrictions on Systems and Data. Users ~~shall~~ must not attempt to gain unauthorized access to data or to breach or evade any security measures on AJIN.

D. Electronic Communication and Internet Technology Management Responsibilities

1. Electronic Communications and Internet Management.

   a. Management. The AOC manages the computers and the AJIN network on which the court's electronic communications and Internet access are conducted, and has certain rights to software and data residing on, developed on, or licensed for the court's computers and networks. AJIN management ~~shall~~ must administer, protect, and monitor the aggregation of computers, software, and networks operating within the AJIN network including those connecting via wireless access points and those traversing AJIN to reach the Internet. AJIN Management may conduct periodic phishing tests to improve employees' security awareness levels.

   b. Use for Court Purposes. The appointing authority ~~shall~~ must ensure, through appropriate policies and procedures, that electronic communications, information technology resources, and Internet access used by courts under the appointing authority's administrative supervision are used to support activities connected with the business of the court.

   c. Use of Software and Data Files. Each user ~~shall~~ must ~~learn~~ strive to use electronic communication software, data files, and Internet resources correctly and efficiently.

d. Equitable Use of Resources. AJIN management ~~shall~~ must manage electronic communications information technology resources, network bandwidth, and Internet access to ensure that users have equitable access to these resources. AJIN management may occasionally need to restrict use of shared communications systems, including requiring users to refrain from using any music streaming, video content, software program, communications practice, or database that is unduly resource intensive.

e. Efficient Use of Resources. Users ~~shall~~ must use electronic communications media and the Internet efficiently, to avoid wasting or overburdening the judicial department's network computing resources. Users ~~shall~~ must accept limitations or restrictions on file storage space, usage time, or amount of resources consumed, when asked to do so by systems administrators. In particular, users ~~shall~~ must carefully consider and appropriately limit the use of ~~groups~~ personal email accounts and "all users" distribution lists to send messages ~~to multiple recipients, sending of~~ or announcements~~, and~~ as well as ~~appending~~ the attachment of large ~~text~~ video or graphics files to messages.

f. Policies and Procedures. Appointing authorities ~~shall~~ must communicate the judicial department's electronic communications, Internet access, information technology policies, security policies, and user responsibilities, systematically and regularly to all their users.

g. Monitoring Effectiveness of Policies and Procedures. AJIN management ~~shall~~ must monitor the application and effectiveness of electronic communications~~, and~~ information technology, and Internet-usage policies~~, and use of the Internet~~ and must propose changes as events or technology warrant.

h. Access to Internet Pornography. Pursuant to A.R.S. § 38-448, all users ~~shall~~ must receive notice and copies of the statute prohibiting access to internet pornography. The appointing authority ~~shall~~ will act as the agency head for granting exceptions.

2. Security and Privacy.

a. Security Procedures. AJIN management ~~shall~~ must establish and support reasonable standards and procedures for security of electronic data and information produced, used, or distributed in the judicial department~~, and~~ to ensure the integrity and accuracy of data the court maintains.

b. Protection Against Unauthorized Use. All users ~~shall~~ must protect AJIN's computers, networks, and data from destruction, tampering, and unauthorized inspection and use. Each user ~~shall~~ must establish ~~appropriate passwords~~ a unique password for the user's account in the first instance, change passwords periodically as may be required by network system administrators, ~~avoid~~ refrain from sharing or disclosing passwords to others ~~except to AJIN management in connection with system administration or~~

~~troubleshooting tasks~~, and prevent unauthorized or inadvertent access by others to their computers and files, including Internet-accessible resources.

c. Protection Against Data Loss. AJIN management ~~shall~~ must ensure that the AJIN's computer systems do not lose important data due to hardware, software, or administrative failures or breakdowns. Authorized systems administrators or technical personnel may occasionally need to examine the contents of particular data files to diagnose or correct problems.

d. Encryption. Under ACJA § 1-505, ~~Only~~ only specified forms of encryption are permitted. AJIN email users may encrypt their electronic mail and files only with the use of software approved by AJIN management. Users ~~shall~~ may use encryption only for specialized transactions and only with express approval of the appointing authority. The encryption key to the software ~~shall~~ must be retained by AJIN management to access encrypted messages, which may limit the degree of privacy protection provided by such encryption.

3. Access and Disclosure.

a. Monitoring of Electronic Communications. AJIN management ~~shall~~ must not engage in the systematic monitoring of electronic ~~mail messages~~ communications, the electronic records created by use of email systems, or other electronic files created by users.

b. Monitoring of Internet Access. AJIN management ~~shall~~ must systematically monitor Internet access and the amount of time spent on the Internet by users. Monitoring ~~shall be~~is primarily for the purpose of supporting the management responsibilities related to the equitable and efficient use of resources, but ~~could also~~ may include monitoring of unlawful activity, conduct that would adversely reflect on the court, or other violation of this section if detected or suspected.

c. Access. AJIN management reserves the right to permit authorized staff to access and disclose the contents of electronic messages~~, provided that it follows appropriate procedures~~, in the course of an investigation triggered by indications of user misconduct, as needed to protect health and safety, ~~as needed to~~ prevent interference with the mission of the courts, ~~to~~ protect system security, comply with legal process, ~~or~~ fulfill court obligations to third parties, protect the rights or property of the courts, or ~~as needed to~~ locate substantive information required for court business that is not more readily available by some other means.

d. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring. The contents of electronic communications, properly obtained for legitimate ~~business~~ court purposes, may be disclosed without permission of the user. The judicial department will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a specific ~~business~~ court purpose, satisfy a legal obligation, or to appropriately respond to

requests for records disclosure under Rule 123 or applicable~~state or federal~~ laws governing ~~public~~ access to records.

4. Public Access and Disclosure.

   a. Public Records. Users ~~shall~~ must store, preserve, and make retrievable electronic ~~mail~~ messages and files according to Rule 123 and applicable law, ~~and~~ policies, and procedures ~~defining~~ governing the public record status of the data. Users ~~shall~~ must consider the use ~~designations~~ categories in paragraph (C.)(1) of this section when creating ~~mail~~ electronic messages, and must understand that materials in all categories could be released to the public if it is determined that the information is ~~not exempt from~~ subject to disclosure.

   b. Public Access to Court Records. Rule 123, ~~Rules of the Supreme Court of Arizona, (as modified or superseded by future rules)or its successor~~ ~~determines~~ governs the public record status of court records and communications and~~. This rule governs~~ access to the records of all courts.

   c. Public Access Address. The judicial department, or AJIN management on its behalf, ~~shall~~ must provide, publish, and maintain an electronic mail address for public access to courts, preserving the confidentiality of judicial officers and court management addresses, as needed, and providing a single point of access for electronic public inquires.

5. Email Records Retention and Disposition.

   a. Records Retention and Disposition. Users ~~shall~~ must retain and dispose of ~~email~~ electronic communications pursuant to ~~an~~ the approved retention schedule and consistent with Rule 123~~, Rules of the Supreme Court of Arizona~~.

   b. Procedures. AJIN management ~~shall~~ must establish or modify, as needed in light of the retention schedule, reasonable standards and procedures for maintaining and purging backups of electronic data and information prepared in or transmitted by an electronic ~~mail~~ communication program or software application.

E. Enforcement.

1. Audit Authorization. When necessary to enforce the judicial department's rules or policies, an authorized administrator may disable network connections by certain computers, require adequate identification of computers and users on the network, undertake audits of software or information on shared systems, or take steps to secure compromised computers that are connected to the network.

2. Disciplinary Action. Users are responsible for any activities that occur using their unique associated credentials. Appropriate disciplinary action will be taken against individuals

found engaging in prohibited use of ~~the AJIN's~~ electronic communications resources. Disciplinary action may include, but is not limited to, loss of access to the electronic communications, computer, or network resources as well as any other appropriate disciplinary action.

3. ~~Non-court~~ Non-Court Users. Prohibited or inappropriate use of AJIN's electronic communications resources by authorized non-court users may result in possible legal sanctions or cancellation of any court contract.

4. Cooperation. Users ~~shall~~ must cooperate with any authorized investigation of technical problems and of possible violations of this section. Failure to do so is grounds for disciplinary ~~measures~~ action.

5. Acknowledgment. Employees, contractors, and volunteers must indicate agreement with the electronic communications policy by signing the attached agreement (or its electronic equivalent).

Acknowledgment of Electronic Communications and Internet Access Policy

I understand that the confidentiality and protection of the Arizona Judicial Department's information is of the utmost importance. I have received, read, and understand the Arizona Judicial Department's Electronic Communications Policy in Arizona Code of Judicial Administration ("ACJA") § 1-503 on the use of electronic communications, information technology resources, and Internet access. ~~and~~ I agree to abide by the terms of ~~that~~ the ~~policy~~Policy.

I understand that all information stored in, transmitted, or received through the Arizona Judicial Information Network's ("AJIN") information systems and work-related resources on the Internet is the property of the Arizona Judicial Department, and is to be used only for authorized purposes. I further understand that authorized representatives of the AOC may monitor the use of AJIN's systems and work-related, Internet-accessible resources from time to time to ensure such use is consistent with the Arizona Judicial Department's ~~policies~~ Electronic Communications Policy ~~and interests~~ and that I can have no expectation of privacy in my electronic communications, Internet access, or any other information stored in, transmitted, or received through AJIN. Further, I am aware that my use of a password or code does not in any way restrict the Arizona Judicial Department's right or ability to access electronic communications.

I have been provided with access to A.R.S. § 38-448 and the Electronic Communications Policy in ACJA § 1-503. I am aware that any violation of the ~~email and Internet access policy~~ Electronic Communications Policy may result in loss of system privileges, possible legal sanctions and, for employees, disciplinary action up to and including termination of employment.

Date: _____

Employee Name: _____

Employee Signature: _____

Division: _____

Department: _____

(Any online version of this acknowledgement must stipulate to the above content even if not worded identically.)