JUDICIAL BRANCH OF MARICOPA COUNTY

Section: **CS-125** Pg. **1** of **11** Attachments _3_	**Original Date:** June 17, 1997
Subject: **ELECTRONIC COMMUNICATIONS POLICY**	New_____Addl _____
Policy **X** Procedure ____ Information _____	REVISION: 5 DATE: 6/18/04
Policy Authority: Presiding Judge; Adopted by Judicial Executive Committee, January 19, 1999, Supreme Court Administrative Order 2003-89; Arizona Supreme Court Rule 123; Revision Adopted by Judicial Executive Committee, June 18, 2004	Related Sections: _____ Authorized Signature(s)

I. INTRODUCTION

This statement sets forth the Judicial Branch (hereafter "Judicial Branch") policy with regard to use of, access to, and management of electronic communication and Internet access. For purposes of this policy statement, "electronic communication" may include but is not limited to electronic mail, Internet services, Intranet services, voice mail, and facsimile messages that are sent or received by Judicial Officers, employees, and other authorized users, and the network resources over which such communications are transmitted. "Internet" may include but is not limited to access to the World Wide Web. Employee use of Judicial Branch computer resources generally is addressed in separate policies.

II. POLICY

A. **Persons Covered by this Policy.** The policy applies to all Judicial Branch Employees, which includes Superior Court and Juvenile Court judicial officers and staff; Superior Court and Juvenile Court administration, Adult and Juvenile Probation employees, Justices of the Peace and Justice Court employees; staff, pool, and contract court reporters and interpreters; and constables.

B. **Purpose.** Electronic communications and Internet technology allows access to a broad range of ideas and information, and facilitates the exchange of ideas and information in a timely and efficient manner. The Judicial Branch supports the use of electronic communications, networked information and Internet resources to further its mission, and to foster communication and information exchange within the Judicial Branch and the justice community. The purpose of this policy is to set forth the guidelines and mutual responsibilities for managing and using the Judicial Branch's electronic communications resources and Internet access. Administration has the responsibility to manage the Judicial Branch electronic communications resources and Internet, and to ensure that the resources are used to support the business of the Judicial Branch through implementation of appropriate policies and procedures. Judicial Branch employees 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 the Judicial Branch provides access.

C. **Authorized Use.** All employees shall use provided electronic communications resources and Internet access responsibly, for purposes relating to the business of the Judicial Branch or enhancing the work environment of the Court, as set forth in this policy.

D. **Authorized Persons.** Only Judicial Branch employees may use the provided electronic communications resources. Specifically designated Judicial Branch employees may use the Judicial Branch's Internet resources. Use of these resources by non-employees requires prior authorization from Administration and Judicial Information Services ("JIS") to maintain network integrity.

E. **Relationship to Other Rules.** Use of computers, electronic communications and Internet resources is subject to all other rules governing the Judicial Branch including the Judicial Merit System Resolution and Rules, Judicial Branch Policies and Procedures, and Arizona Supreme Court Rule 123 governing public access to judicial records. Statements in this policy regarding permissible and prohibited uses of computers, electronic communications and the Internet are intended as additional guidelines and examples.

To the extent that electronic communications policies of the Judicial Branch conflict with County or other governmental branch electronic communications policies, Judicial Branch policies and procedures control and shall be followed.

F. **Employees' Personal Computers.** Employees who choose to bring their own personal computers to work, are subject to these policies as well. Employees who bring their own personal computers to work are prohibited from attaching those computers to the network infrastructure.

III. RESPONSIBLE USE OF ELECTRONIC COMMUNICATIONS AND INTERNET RESOURCES

A. Guidelines for Responsible Use of Electronic Communications.

1. **Professionalism.** Electronic communications shall be professional and business-like. Electronic mail messages, whether sent within the Judicial Branch or outside the Judicial Branch, should withstand public scrutiny without embarrassment to the Judicial Branch, other employees, and the public.

2. **Professional Use.** It is permissible to use provided e-mail systems for limited professional purposes with supervisor approval. Approved professional uses may include participation in professional associations, continuing education, scholarly publication, communications with colleagues, and subscription to listservs, news groups or topical updating services related to the Judicial Branch, the judicial branch, or an employee's professional duties. Employees subscribing to such services shall keep up with the mail received, regularly delete messages once read, learn the rules associated with the service and know how to unsubscribe (both for ending participation and for absences such as vacation), and maintain a professional demeanor when posting to a list. Such use is in all respects subject to approval of the employee's supervisor.

3. **Routine Use.**

a. Routine communications may include: scheduling meetings; requests for information; the assignment of work tasks or clarification of assignments; notification of employees' whereabouts such as sick days or vacation requests.

b. Personal use. It is permissible to use the provided electronic communications systems for occasional personal purposes. Occasional personal uses may include notifying family members of schedule changes, personal messages to co-workers, and other uses typically permitted to be communicated in or from the workplace in person or by telephone. Such use does not include uses requiring substantial expenditure of workplace time, uses for profit or for personal charitable or political solicitations or campaigns, or uses that would otherwise violate Judicial Branch policies with regard to employee time commitments or Judicial Branch equipment. It is the responsibility of the employee sending such messages to ensure that the message is identified, either specifically or clearly by its content, as personal in nature, and not on behalf of the Judicial Branch. Such use is in all respects subject to approval of the employee's supervisor.

4. Formal use. Formal communication is a communication of any kind pertaining to public business, which must be preserved as a record of official action or policy (i.e., policies, decisions, procedures, or other activities of the government). Formal communications may be transmitted via e-mail as long as they are created and preserved in a word processing system. While e-mail is considered public record, IT should not be used to create or store formal communications.

5. Use of Electronic Bulletin Board (E-bulletin Board). The Judicial Branch has developed an electronic bulletin board on the Judicial Branch Intranet for use by staff to broadcast general messages to Judicial Branch employees that are inappropriate for e-mail. Such messages may include items for sale by employees, bake sales, retirement parties, and other information that are not prohibited uses for electronic communications outlined in this policy.

6. Incoming Messages. Messages originating outside the Judicial Branch are in all respects the responsibility of the employee receiving the message. The Judicial Branch may not be held responsible for messages originating outside the Judicial Branch received by employees.

B. Prohibited Uses for Electronic Communications.

1. Commercial Purposes. Employees may not use electronic communications, other than the employee e-bulletin board, for commercial purposes, to promote personal business interests, or for monetary gain. Employees may not send "serial" or "chain" messages on e-mail or the e-bulletin board.

2. Copyright and Intellectual Property Rights. Employees shall 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.

3. Harassment. Employees shall not use electronic communications to intimidate or harass others, or to interfere with the ability of others to conduct Judicial Branch business. Employees shall not use electronic communications in a manner that promotes discrimination on the basis of race, creed, color, gender, religion, disability, or sexual preference.

4. **Other Prohibited Uses.** Users shall not use the Internet access provided by the Judicial Branch for connecting to, posting, downloading or printing pornographic, offensive, or other material that is inappropriate for the workplace, or violates the code of conduct, equal employment opportunity, sexual harassment or A.R.S. §38-448. (See addendum "A" at the end of this policy.) Those employees who have a specific job-related need to access prohibited materials via Judicial Branch computing resources must submit a "request to access prohibited materials detailing the reasons for the requested access and the expected duration of the requested access. The request for access to prohibited materials must be approved by the department head, with final approval by the agency head, prior to submission to JIS. (See addendum "C".)

5. **Identification.** Users shall clearly identify themselves in any electronic communication, and shall not construct an electronic message or communication so as to appear to be from anyone other than the user.

6. **Unauthorized Access**. Employees may not capture and "open" electronic communications except as required in order for authorized employees to diagnose and correct delivery problems, and may not obtain access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial business purpose.

7. **Confidentiality.** Even though employees routinely use e-mail as a form of communication to discuss ideas and pending cases, this form of communication cannot be considered secure and no message should be considered absolutely confidential. It is the employee's responsibility to carefully consider the confidentiality requirements of an electronic communication before it is transmitted. Employees should not send confidential or privileged information, whether formal or routine, via electronic mail, without prior express approval from their supervisor. The confidential or privileged status of a communication is determined by court rule or order, or by statute, and may include such matters as communications relating to employee performance or discipline, and judicial or attorney work product. Anyone using Judicial Branch or County computing resources should have no expectation of privacy in the use of these tools or any content therein.

8. **Software.** Employees may not use Judicial Branch electronic messaging or communications systems to download software, unless they comply with established policies for approval of loading or operating software on Judicial Branch-provided computers, verification of proper licensing, and scanning for computer viruses which is facilitated through JIS. Installation of software on computers by employees outside of JIS is strictly prohibited unless made available by JIS or otherwise approved for installation by JIS.

9. **Adherence to Security Restrictions on Systems and Data.** Employees shall 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.

C. Guidelines for Responsible Use of the Internet:

1. Professionalism. Internet use shall be professional and business-like. Such use should withstand public scrutiny without embarrassment to, the Judicial Branch, other employees, and the public.

2. Professional Use. It is permissible to use the Judicial Branch's Internet access for limited professional purposes with supervisor approval. Approved professional uses may include participation in professional associations, continuing education, scholarly publication, legal research related to, the Judicial Branch, or an employee's professional duties. Such use is in all respects subject to approval of the employee's supervisor.

3. Routine Use.

a. Routine use may include, but is not limited to: locating information on a particular topic for work-related use; accessing other courts' information and sites; and, accessing information by various professional organizations.

b. It is permissible to use the Judicial Branch's Internet resources for occasional personal purposes. Occasional personal uses may include using the Internet for the location of information relating to personal interests. Such use does not include uses requiring substantial expenditure of workplace time, uses for profit or for personal charitable or political solicitations or campaigns, or uses that would otherwise violate Judicial Branch policies with regard to employee time commitments or Judicial Branch equipment. It is the responsibility of the employee using the Internet to ensure that the use complies with all current policies. Such use is in all respects subject to approval of the employee's supervisor.

D. Prohibited Uses Regarding the Internet.

1. Commercial Purposes. Employees may not use the Internet for commercial purposes, to promote personal business interests, or for monetary gain.

2. Copyright and Intellectual Property Rights. Employees shall not use the Internet resources provided by the Judicial Branch in violation of copyright laws, or to download or receive software in violation of intellectual property laws or rights.

3. Harassment. Employees shall not use the Internet access provided by the Judicial Branch to intimidate or harass others, or to interfere with the ability of others to conduct Judicial Branch business. Employees shall not use the Internet access provided by the Judicial Branch in a manner that promotes discrimination on the basis of race, creed, color, gender, religion, disability, or sexual preference.

4. OTHER PROHIBITED USES.

Users shall not use the Internet access provided by the Judicial Branch for connecting to, posting, downloading or printing pornographic, offensive, or other material that is inappropriate for the workplace, or violates the code of conduct, equal employment opportunity, and sexual harassment of A.R.S. §38-448.

(See Addendum "A" at the end of this policy.) Those employees who have a specific job-related need to access prohibited materials using Judicial Branch computing resources must submit a "request to access prohibited materials" detailing the reasons for the requested access and the expected duration of the requested access. The request for access must be approved by the department head, with final approval by the agency head, prior to submission to JIS. (See addendum "C".)

5. **Software.** Employees may not use the provided Internet access to download software unless they comply with established policies for approval of loading or operating software on Judicial Branch provided computers, verification of proper licensing, and scanning for computer viruses, which is facilitated by JIS. Installation of software on Computers by employees outside of JIS is strictly prohibited unless made available by JIS or otherwise approved for installation by JIS.

6. **Unauthorized Access.** Employees may not obtain access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial business purpose.

7. **Adherence to Security Restrictions on Systems and Data.** Employees shall not attempt to gain unauthorized access to data or breach or evade any security measures.

EXAMPLES OF UNACCEPTABLE USE:
(THE FOLLOWING PROVIDES SOME EXAMPLES OF IMPROPER USES OF JUDICIAL BRANCH AND COUNTY COMPUTING RESOURCES. IMPROPER USAGE IS NOT LIMITED TO THESE EXAMPLES.)

- Use of Judicial Branch or County Computing Resources to conduct commercial or private business transactions, or support a commercial or private business other than County business (e.g. using judicial branch -supplied personal computers to prepare transcripts for sale; using fax machines or telephones to further an employee's commercial/private business endeavors).
- Use of Judicial Branch or County Computing Resources to promote fundraising or advertising of non-County organizations that have not been pre-approved.
- Downloading or copying of data, software, or music that is not authorized or licensed.
- Performing gambling activities or other illegal schemes (e.g. pyramid, chain letters, etc.)
- Disclosing protected Judicial Branch or County data (confidential, private, or best interest) via Judicial Branch or County Computing Resources without proper authority.
- Misrepresenting another user's identification (forging or acting as), or gaining or seeking to gain non-authorized access to another user's account/data or the passwords of other users, or vandalizing another user's data.
- Generating or possessing material that is considered harassing, obscene, profane, intimidating or threatening, defamatory to a person or class of persons, or otherwise inappropriate or unlawful, including such material that is intended only as a joke or for amusement purposes.
- Failure to comply with instructions from appropriate Judicial Branch or County staff to discontinue activities that threaten the operation or integrity of the Judicial Branch or County Computing Resources, or are deemed inappropriate, or otherwise violate this policy.

IV. INTERNET AND ELECTRONIC COMMUNICATIONS TECHNOLOGY MANAGEMENT RESPONSIBILITIES

A. Electronic Communications and Internet Management.

1. **Management.** The Judicial Branch acquires and deploys the computers and the internal computer networks on which the Judicial Branch's 's electronic communications and Internet access are conducted, cooperates with Maricopa County in using and administering the internal computer networks, and has certain rights to the software and data residing on, developed on, or licensed for Judicial Branch's computers and networks, JIS which includes Justice Court Automation (JCA) and Research and Planning Services (RAPS) HAS the responsibility to administer, protect, and monitor the aggregation of computers, software, and networks.

2. **Use for Court Purposes.** The Presiding Judge has the responsibility of ensuring, through appropriate policies and procedures, that electronic communications information technology resources and Internet access are used to support activities connected with the business of the Judicial Branch.

3. **Use of Software and Data Files.** It is the responsibility of each user to learn to use electronic communications software and Internet resources correctly and efficiently.

4. **Equitable Use of Resources.** JIS, network administrators have the responsibility to manage electronic communications information technology resources and the Judicial Branch's Internet access so that members of the Judicial Branch community benefit equitably from their use. Authorized staff may occasionally need to restrict inequitable use of shared communication systems, including requiring users to refrain from using any software program, communications practice, or database that is unduly resource-intensive.

5. **Efficient Use of Resources.** It is the responsibility of each employee to use electronic communications media and the Internet efficiently, to avoid wasting or overburdening Judicial Branch computing resources. Users should 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 should carefully consider and appropriately limit the use of groups to send messages to multiple recipients, sending of announcements, and appending large text or graphics files.

6. **Policies and Procedures.** Supervisors have the responsibility to communicate Judicial Branch electronic communications, Internet access information technology policies, and employee responsibilities, systematically and regularly to all of their employees.

7. **Monitoring Effectiveness of Policies and Procedures.** Administration has the responsibility to monitor the application and effectiveness of electronic communications information technology policies, and Internet use, and propose changes in policy as events or technology warrant.

8. **ACCESS TO INTERNET PORNOGRAPHY.** Pursuant to A.R.S. §38-448, all users shall receive notice and copies of the statute prohibiting access to Internet

pornography. The appointing authority shall act as the agency head for granting exceptions. (See Addendum "A".)

Those employees who have a specific job-related need to access prohibited materials via Judicial Branch computing resources must submit a "Request to access prohibited materials" detailing the reasons for the requested access and the expected duration of the requested access. The request for access to prohibited materials must be approved by the department head, with final approval by the agency head, prior to submission to JIS. (See Addendum "C".)

B. Security and Privacy.

1. Security Procedures. JIS network administrators have the responsibility to establish and support reasonable standards and procedures for security of electronic data and information produced, used, or distributed in the Judicial Branch, and to ensure the integrity and accuracy of data the Judicial Branch maintains. These administrators have the responsibility to establish and communicate reasonable standards and procedures describing the extent of privacy that employees can expect in the use of networked computer resources.

JIS network administrators have the responsibility of initiating the approved Judicial Branch "acceptable use" banner for all entry points into Judicial Branch computing resources (see Addendum "B" - "Maricopa County Judicial Branch Acceptable Use Banner" that includes a link to this policy - **CS-125 - Electronic Communications Policy**).

2. Protection Against Unauthorized Use. All Judicial Branch employees have the responsibility to protect Judicial Branch computers, networks and data from destruction, tampering, and unauthorized inspection and use. It is the responsibility of each user to establish appropriate passwords for the user's account in the first instance, to change passwords periodically as may be required by network system administrators, to avoid sharing or disclosing passwords to others, and to prevent unauthorized or inadvertent access by others to their computers and files.

3. Protection Against Data Loss. Network administrators have the responsibility to ensure that Judicial Branch computer systems do not lose important data due to hardware, software, or administrative failures or breakdowns.

4. Encryption. Only specified forms of encryption are permitted. Judicial Branch employees may encrypt their electronic mail and files only with the use of software approved by JIS. Encryption may only be used for specialized transactions and only with express approval by Administration. The encryption key to the software must be retained by JIS to access encrypted messages, which may limit the degree of privacy protection provided by such encryption.

C. Access and Disclosure.

1. Monitoring of Electronic Communications. The Judicial Branch will not engage in the systematic monitoring of electronic mail messages, the electronic records created by use of e-mail systems, or other electronic files created by employees.

2. **Monitoring Internet Access.** The Judicial Branch may engage in the systematic monitoring of Internet access and amount of time spent on the Internet by employees.

3. **Access.** The Judicial Branch 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 employee misconduct, as needed to protect health and safety, as needed to prevent interference with the mission of the Judicial Branch, to protect system security, comply with legal process or fulfill Judicial Branch obligations to third parties, protect the rights or property of the Judicial Branch , or as needed to locate substantive information required for Judicial Branch business that is not more readily available by some other means.

4. **Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring.** The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee. The Judicial Branch 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 purpose, satisfy a legal obligation, or to appropriately respond to requests for records disclosure under state or federal laws governing public access to records.

D. Public Access and Disclosure.

1. **Public Records.** Electronic mail messages and files should be stored, preserved, and made retrievable according to law and policies and procedures defining the public record status of the data. The designations in section III(A) of this policy should be kept in mind when creating e-mail messages, but materials in all categories could be released to the public if it is determined that the information is not exempt from disclosure.

2. **Public Access to Judicial Records.** The public record status of court records and communications is determined by Arizona Supreme Court Rule 123, Public Access to the Judicial Records of the State of Arizona. (Hereafter "Rule 123.) This rule governs access to the records of all court and administrative offices of the judicial department of the State of Arizona.

   a. **Definition.** Rule 123 defines a record as: "all existing documents, papers, letters, maps, books, tapes, photographs, films, sound recordings or other materials, regardless of physical form or characteristics, made or received pursuant to law or in connection with the transaction of any official business by the court, and preserved or appropriate for preservation by the court as evidence of the organization, functions, policies, decision, procedures, operations or other governmental activities." This ruler applies to all computer or electronic-based records maintained by the Court, including e-mail.

   b. **Access.** Records of all courts and administrative offices of the Judicial Department of the State of Arizona are presumed to be open to any member of the public for inspection or copying at all times during regular business hours at the office having custody of the records except as may be closed by law. In the view of the possible countervailing interests of confidentiality, privacy or the best interests of the state, public access to

some records may be restricted or expanded in accordance with the provisions of Rule 123 and other provisions of law

c. **Closed Records.** A closed record means that the public may not inspect, copy, or otherwise have access to such record, except by Court order. Closed records may be released to the public once all confidential information has been redacted unless release of the entire record is prohibited by law. Records prepared in or transmitted by electronic mail have the same public record status as a paper-copy equivalent would have under Rule 123. For example, records and communications constituting judicial work product and drafts, notes, memoranda or drafts thereof prepared by a judge or other court personnel at the direction of or for a judge and used in the process of preparing a final decision or in the course of deliberations on rule or administrative matters, are closed.

d. **Segregation.** Whenever possible, employees generating or receiving data or information that could be considered closed or confidential pursuant to Rule 123 should segregate such information from the remaining public "open" data and information. Employees should clearly label or identify such closed or confidential data and information as confidential.

e. **Requests Shall be Made to:** All public access to judicial records shall be made to the Public Affairs Director of the Judicial Branch, currently J.W. Brown.

f. **Determining Judge.** If the Public Affairs Director determines that there is a question whether records requested to be made available for public inspection should be disclosed, or if a request is made for a ruling by a judge following denial of a request to inspect records, the Public Affairs Director shall refer the request to the presiding judge, or a judge authorized in writing by the presiding judge, for determination. The presiding judge may assert any applicable privilege or objection should a public records or discovery request be made regarding any electronic communication. Assertions of privilege or objections may be made only by the presiding judge, or a judge authorized in writing by the presiding judge.

3. **Public Access Address.** The Court shall publish and maintain an electronic mail address for public access to the Court, preserving the confidentiality of judicial officer and Court management addresses as needed and providing a single point of access for electronic public inquiries.

E. E-mail Records Retention and Disposition.

1. **Records Retention and Disposition.** E-mail communications will be retained and disposed of pursuant to this policy. E-mail that has not been completely deleted from all containers (e.g., in-box, folders, etc.) and by all recipients, system e-mail directories, and system distribution lists will be backed up on tape nightly. All e-mail system back-up tapes will be retained and overwritten on a 28-day back-up cycle; i.e., the 29th day will overwrite the first tape, the 30th day overwrites the second tape, etc.

2. **Department Policies.** Court departments may establish more stringent retention and disposition policies to meet unique security needs, consistent with the public record requirements of Rule 123.

3. **Procedures.** JIS network administrators have the responsibility to establish or modify as needed in light of the foregoing retention schedule, reasonable standards and procedures for maintaining and purging backups of electronic data and information prepared in or transmitted by electronic mail.

V. POLICY ENFORCEMENT

A. When necessary to enforce Judicial Branch 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.

B. Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of Judicial Branch electronic communications resources. Such action may include, but is not limited to, loss of access to electronic communications, computer, or network resources, and any action appropriately imposed under the Judicial Merit System Resolution and Rules.

C. Users are expected to cooperate with authorized investigation of technical problems, and of possible unauthorized or irresponsible use as defined in this policy. Failure to do so may be grounds for disciplinary measures

EMPLOYEE ACKNOWLEDGEMENT

I have received copies of the Electronic Communications Policy, CS-125 AND A.R.S. §38-448.

I am aware that any violation of the **Electronic Communications Policy** may result in loss of system privileges, possible legal sanctions, and, for employees, disciplinary action up to and including termination.

_____
Employee's name - Please print

_____
Employee's signature

_____
Date

_____
Court Department Representative

ADDENDUM "A"

Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 38, chapter 3, article 4, Arizona Revised Statutes, is amended by adding section 38-448, to read:

38-448. State employees; access to internet pornography prohibited; cause for dismissal; definitions

A. EXCEPT TO THE EXTENT REQUIRED IN CONJUNCTION WITH A BONA FIDE, AGENCY APPROVED RESEARCH PROJECT OR OTHER AGENCY APPROVED UNDERTAKING, AN EMPLOYEE OF AN AGENCY SHALL NOT KNOWINGLY USE AGENCY OWNED OR AGENCY LEASED COMPUTER EQUIPMENT TO ACCESS, DOWNLOAD, PRINT OR STORE ANY INFORMATION INFRASTRUCTURE FILES OR SERVICES THAT DEPICT NUDITY, SEXUAL ACTIVITY, SEXUAL EXCITEMENT OR ULTIMATE SEXUAL ACTS AS DEFINED IN SECTION 13-3501. AGENCY HEADS SHALL GIVE, IN WRITING, ANY AGENCY APPROVALS. AGENCY APPROVALS ARE AVAILABLE FOR PUBLIC INSPECTION PURSUANT TO SECTION 39-121.

B. AN EMPLOYEE WHO VIOLATES THIS SECTION PERFORMS AN ACT THAT IS CAUSE FOR DISCIPLINE OR DISMISSAL OF THE EMPLOYEE AND FOR AN EMPLOYEE IN STATE SERVICE IS CONSIDERED MISUSE OR UNAUTHORIZED USE OF STATE PROPERTY PURSUANT TO SECTION 41-770.

C. ALL AGENCIES SHALL IMMEDIATELY FURNISH THEIR CURRENT EMPLOYEES WITH COPIES OF THIS SECTION. ALL AGENCIES SHALL FURNISH ALL NEW EMPLOYEES WITH COPIES OF THIS SECTION AT THE TIME OF AUTHORIZING AN EMPLOYEE TO USE AN AGENCY COMPUTER.

D. FOR THE PURPOSES OF THIS SECTION:

1. "AGENCY" MEANS:

(a) ALL OFFICES, AGENCIES, DEPARTMENTS, BOARDS, COUNCILS OR COMMISSIONS OF THIS STATE.

(b) ALL STATE UNIVERSITIES.

(c) ALL COMMUNITY COLLEGE DISTRICTS.

(d) ALL LEGISLATIVE AGENCIES.

(e) ALL DEPARTMENTS OR AGENCIES OF THE STATE SUPREME COURT OR THE COURT OF APPEALS.

2. "INFORMATION INFRASTRUCTURE" MEANS TELECOMMUNICATIONS, CABLE AND COMPUTER NETWORKS AND INCLUDES THE INTERNET, THE WORLDWIDE WEB, USENET, BULLETIN BOARD SYSTEMS, ON-LINE SYSTEMS AND TELEPHONE NETWORKS.

ADDENDUM "B"

MARICOPA COUNTY TRIAL COURTS ACCEPTABLE USE BANNER

Acceptable Use Statement

By logging into and/or using Judicial Branch Computing Resources, I acknowledge that I have read, understand, agree, and will comply with the current Judicial Branch policy, **CS-125 - Electronic Communications Policy**. My usage will be monitored for compliance and I accept all liabilities associated with any misuse on my part."

ADDENDUM "C"

MARICOPA COUNTY JUDICIAL BRANCH
Request to Access Prohibited Materials
Via Judicial Branch Computing Resources

Employee Name: _____

Date of Request: _____

Internet site(s) or information infrastructure to accessed or used: _____

_____

_____

Expected duration of need to access or use Internet site(s) or information infrastructure containing prohibited materials: _____

_____

Reasons for access or used: _____

_____

_____

By logging into and/or using Judicial Branch Computing Resources, I acknowledge that I have read, understand, agree, and will comply with the current Judicial Branch policy, **CS-125 – Electronic Communications Policy**. My usage will be monitored for compliance and I accept all liabilities associated with any misuse on my part.

_____ _____

Signature of Requesting Party Date

I hereby acknowledge that the requesting employee has a legitimate reason for accessing prohibited materials via Judicial Branch computing resources. The reason for the requested access has been accurately described and I approve said access for limited purposes only as detailed above.

_____ _____

Signature of Department Head Date

APPROVAL OF AGENCY HEAD OR APPOINTING AUTHORITY:

_____ _____

Signature of Agency Head Date

JUDICIAL INFORMATION SYSTEMS:

_____ _____

Received and Processed By Date