## TELEPHONES AND OTHER COURT TECHNOLOGY RESOURCES

### A. Business Use Policy

**The Court provides telephones, electronic mail and other electronic resources to employees to assist them in performing their jobs. The Court therefore, incorporates into this manual the Georgia Technology Authority's policy on use of Information Technology Resources as summarized below. In addition, the Court reserves the right to monitor business-related telephone calls and electronic mail messages conducted in the workplace as well as to retrieve and read any data composed, transmitted or received through online connections and/or stored on Court servers or other Court property.**

### B. Personal Use

**Occasional personal use of the telephone, Internet connectivity and email that do not involve any inappropriate use as described below is permitted by the Court. Any such use should be brief, infrequent and should not interfere with the employee's job performance, duties or responsibilities.** It is preferable that employees make such necessary personal calls or send email messages during their 15 minute breaks, but in no case should personal calls exceed 15 minutes in a day. Violation of this policy will result in disciplinary action. No personal long distance calls shall be made on office telephones unless charged to the employee's personal credit card or home telephone account.

### C. Inappropriate Use

**Inappropriate use of technology resources includes, but is not limited to:**

(1) **Conducting private or personal for-profit activities.**

(2) **Conducting unauthorized not-for-profit business activities.**

(3) **Conducting any illegal activities as defined by Federal, State and local laws or regulations.**

(4) **Creating, accessing or transmitting sexually explicit, obscene or pornographic material.**

(5) **Creating, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing or intimidating.**

(6) **Creating, accessing or participating in online gambling.**

(7) **Infringing of any copyright, trademark, patent or other intellectual property right.**

(8) **Performing any activity that could reduce the security of the system/network, degrade the system/network performance or cause the loss of, corruption of, or prevent full access to data.**

(9) **Attempting to modify or remove computer equipment, software or peripherals without proper authorization.**

(10) **Attempting to libel or otherwise defame any person.**

(11) **Using another employee's access for any reason unless explicitly authorized.**

(12) **Conducting any activity or solicitation for political or religious causes.**

(13) **Distributing State data and information without authorization.**

**An attempt to use technology resources inappropriately will be treated in the same manner as the actual use of the resources inappropriately.**

**Violation of the Court or State policy on the use of technology resources may result in disciplinary action, termination or criminal prosecution.**

D. No Court equipment is to be used for viewing pornographic or salacious material, sending or receiving same, except as may be necessary in the review of issues on appeal.

| GTA | Georgia Technology Authority | |
|---|---|---|
| **Title:** | **Appropriate Use of Information Technology Resources** | |
| **PSG Number:** | P-08-003.01 | **Topical Area:** Security |
| **Document Type:** | Policy | **Pages:** 4 |
| **Issue Date:** | 3/20/08 | **Effective Date:** 3/20/08 |
| **POC for Changes:** | GTA Office of Information Security | |
| **Synopsis:** | Establishes an enterprise policy regarding appropriate use of State of Georgia information technology (IT) resources. | |

## PURPOSE

State of Georgia information technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to state government policies and applicable state and federal laws. It is the responsibility of Users to ensure that such resources are not misused.

## SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (Policy)

## POLICY

State information technology resources are tools to be used to facilitate the execution of official state business. The use of such resources imposes certain responsibilities and obligations on Users and is subject to state government policies and applicable state and federal laws. Users of State information technology resources shall refrain from inappropriate use (as defined in Terms and Definitions) of such resources at all times, including during breaks or outside of regular business hours.

## RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Appropriate Use and Monitoring (Standard)
Electronic Communications Accountability (Standard)
Email Use and Protection (Standard)

## TERMS and DEFINITIONS

**Information Technology Resources or IT Resources** means hardware, software, and communications equipment, including, but not limited to:
personal computers, email, internet, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities), and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

**Inappropriate usage** includes (but is not limited to) actual or attempted misuse of information technology resources for:

- Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- Conducting unauthorized not-for-profit business activities;
- Conducting any illegal activities as defined by federal, state, and local laws or
- regulations;
- Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;
- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance;
- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of state data and information;
- Attempts to subvert the security of any state or other network or network
- resources;
- Use of another employee's access for any reason unless explicitly authorized;
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.
- Attempts to libel or otherwise defame any person

# Court of Appeals

Memorandum

---

**To:** All judges and all court staff

**From:** Chief Judge Smith

**Subject:** State policy on IT resources

**Date:** July 1, 2003

---

The attached memoranda come from Bud Tirey and Technical Support. They remind us of the basic policies and limitations on appropriate use of our court's computers and other information technology resources. As noted, these are the state's minimum policies and limitations. Our court's IT resources are also subject to policies, procedures, and limitations set by the court, particularly with respect to issues affecting confidentiality.

Please advise in writing if you have any questions or any suggestions as to clarification or improvement of court policy in this area.

attachments

**OFFICE OF THE STATE INSPECTOR GENERAL**

**SONNY PERDUE**
Governor

June 27, 2003

**JAMES E. SEHORN**
State Inspector General

**MEMORANDUM**

**TO:** Agency Heads

**FROM:** James E. Sehorn, Georgia State Inspector General

Tom Wade, Acting Executive Director
Georgia Technology Authority

**RE:** State Policy on Appropriate Use of Information Technology Resources

The state of Georgia provides computers and other technology to its employees so they can conduct work-related duties. In turn, employees are responsible for using technology for legitimate work-related purposes. We are asking you to ensure that your agency's employees understand and follow the provisions of the state policy on appropriate use of information technology resources. A copy of the policy is enclosed.

Among the activities prohibited by the policy are:

- business transactions for the personal gain of a state employee;
- activities in violation of federal, state or local laws and regulations;
- creating, accessing or transmitting materials considered sexually explicit or pornographic, discriminatory, offensive, threatening, harassing or intimidating;
- gambling;
- unauthorized distribution of state data and information; and
- compromising the security of an agency's or the state's data network.

Agencies may establish more stringent policies and procedures regarding their employees' use of IT resources, including the Internet and e-mail. Please assist your employees in understanding and complying with the policy. For instance, stress to your employees that when they use any computer at work, they should have no expectation of privacy. These communications are considered to be state property and may be examined by management for any reason including, but not limited to, security and/or employee conduct. In addition, agencies are responsible for preventing improper disclosure of personal information entrusted to them by Georgia residents. Employees should also understand that violating the policy could result in disciplinary actions, including dismissal and criminal prosecution.

The role of the Office of Inspector General includes taking measures to prevent fraud, waste, abuse and corruption. We are bringing the policy on appropriate use of IT resources to your attention at this time as a preventive measure. As leaders of state government, we all must be concerned about preventing the misuse and abuse of the taxpayers' resources. This would certainly include the state's considerable investment in information technology.

We appreciate your assistance in this effort. Feel free to contact us if you have questions or comments.

Enclosure

2 Martin Luther King, Jr. Drive, SW • 1102 West Tower • Atlanta, Georgia 30334
Phone: 404.656.7924 • Toll-Free 866.435.7644 • Fax: 404.657.9716

Georgia Technology Authority

# Appropriate Use of Information Technology Resources

| POLICY NUMBER: 3.1.3 | EFFECTIVE DATE: 09/10/02 |
|---|---|

## PURPOSE

To establish an enterprise policy regarding appropriate use of State of Georgia information technology (IT) resources.

## SCOPE

All Agencies of the State of Georgia. This policy applies to all employees, contractors, vendors, customers, and others who utilize, possess or have access to State of Georgia IT resources.

## POLICY

***State of Georgia information technology resources are provided to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on Users and is subject to state government policies and applicable state and federal laws. It is the responsibility of Users to ensure that such resources are not misused.***

## STANDARDS

- **To comply with this policy, Users shall refrain from inappropriate use of State of Georgia information technology resources at all times, including during breaks or outside of regular business hours.**

- Inappropriate usage includes (but is not limited to) actual or attempted usage of information technology resources for:

  - Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;

  - Conducting unauthorized not-for-profit business activities;

  - Conducting any illegal activities as defined by federal, state, and local laws or regulations;

  - Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;

- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance;
- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of state data and information;
- Attempts to subvert the security of any state or other network or network resources;
- Use of another employee's access for any reason unless explicitly authorized; or,
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.
- Attempts to libel or otherwise defame any person

- Agencies may establish more stringent policies and procedures consistent with this Enterprise Policy and associated Standards.
- Each Agency reserves the right to retrieve and read any data composed, transmitted or received through online connections and/or stored on their respective servers and /or property. (See enterprise security policy 8.7.3).

## GUIDELINES

State Agencies provide IT equipment as necessary to employees and others for the efficient and effective performance of their duties. IT equipment is provided to carry out job duties, facilitate business-related research and access to information, and also to enhance communication with customers, vendors, colleagues and others receiving services/products from, doing business with, or seeking information from the State.

Occasional personal use of Internet connectivity and e-mail that do not involve any inappropriate use as described above may occur, if permitted by the Agency. Any such use should be brief, infrequent, and shall not interfere with User's performance, duties and responsibilities.

## AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

- Violations of this Policy and associated Standards may result in disciplinary action, termination, or criminal prosecution.

- Occasional access to information or websites of the Georgia Lottery Corporation shall not constitute nor be considered inappropriate use.

**TERMS AND DEFINITIONS** (see Section 2)

**"Information Technology Resources" or "IT Resources"** means hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

## CONFIDENTIAL COMPANY INFORMATION AND INTERNET, COMPUTER, VOICE AND EMAIL POLICY

***Introduction.*** Certain employees may be provided with access to the Internet to assist them in performing their jobs. The Internet can be a valuable source of information and research. In addition, electronic mail can provide an excellent means of communicating with other employees, customers and clients, outside vendors, and other businesses. Additionally, employees often will be privy to confidential Company information in the course of performing their jobs. Use of all this information, however, must be tempered with common sense and good judgment. Accordingly, the Company has formulated the following guidelines to establish the appropriate parameters for the use of Company property and information. This policy will be administered in conjunction with the Company's EEO policy regarding inappropriate or offensive communications and supersedes any and all prior written policies or verbal authorization granted by any individual within the organization.

***Protecting confidential information.*** Protecting our Company's information is the responsibility of every employee, and we all share a common interest in making sure this information is not improperly or accidentally disclosed. Do not discuss the Company's confidential business with co-workers, unless appropriate, or anyone who does not work for us. Employees may not copy or transmit copyrighted material that is not authorized to be sent, trade secrets of the Company or other entities, or proprietary financial or business operations information of the Company or other entities. Additionally, Company communications and property are confidential. Any employee who accesses another person's computer, voice mail, computer file or data, or property without prior approval by an appropriate officer of the Company will be in violation of this policy.

***Business use.*** Employees should keep personal records and personal business at home. All Company equipment and property, including desks, other physical items, computer systems, computer software, diskettes, electronic mail, and voice mail, should be used appropriately for the business of the Company only. These resources are established, maintained, and

provided by the Company for employees to use for the furtherance of the purpose of the Company and not for personal use.

***Disclaimer of liability for use of the Internet.*** The Company is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk.

***Employee's duty of care.*** Employees should endeavor to make each electronic communication truthful and accurate. Employees should use the same care in drafting electronic mail and other electronic documents as they would for any other written communication. Please keep in mind that anything created or stored on the computer system may be and likely will be reviewed by others.

***Duty not to waste computer resources.*** Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, using Company equipment for outside organizations or commercial ventures, selling Internet or other carrier access time, or otherwise creating unnecessary network traffic. Because audio, video, and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related.

***No expectation of privacy.*** Employees should not have an expectation of privacy or security in electronic communications or anything else they create, store, send, or receive on the computer or telephone system. The computers, computer accounts, and telephones given to employees are to assist them in performance of their jobs. By placing information on the Company's systems, employees grant the Company the right to edit, delete, copy,

republish, and/or distribute such information. In addition, electronic mail may be stored indefinitely on any number of computers, including that of the recipient, and may be sent to nonexistent or incorrect user names may be delivered to persons that you never intended. Copies of these messages may be forwarded to others either electronically or on paper.

***Passwords.*** Passwords are designed to give employees access to all or part of the Company's computer, electronic, and/or telephone systems; they are not designed to guarantee the confidentiality of any message or document. The Company retains the right to enter these systems in its sole discretion.

***Monitoring and accessing employee electronic and telephone transmissions.*** The Company at all times retains the right to access, search, and monitor all directories, indices, diskettes, files, databases, electronic mail messages, voice mail messages, Internet sites visited by employees, chat groups and newsgroups, material downloaded or uploaded by users to the Internet, or any other electronic or telephonic transmissions contained in or used in conjunction with the Company's computer, electronic mail, and voice mail systems and equipment with no prior notice. This right applies both during employees' employment by the Company and after its cessation for any reason or no reason, including whether the cessation is voluntary or involuntary. Additionally, computer, electronic mail, and voice mail messages that have been deleted or erased by employees may remain stored in the Company's computer or telephone system. Accordingly, the Company retains the right to access computer, electronic mail, and voice mail messages for as long as the information may be obtained from any source, even after employee has deleted or erased it.

***Blocking of inappropriate content.*** The company may use software or hardware to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by company networks. In the event employees do encounter inappropriate or sexually explicit material while browsing on the Internet, they should disconnect immediately from the site, regardless of whether the site was subject to Company blocking software.

***Prohibited activities.*** Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, violative of the Company's EEO Policy, or otherwise unlawful or inappropriate may not be sent by electronic mail or other forms of electronic communication (*e.g.*, bulletin board systems, newsgroups, groups, chat groups), downloaded from the Internet, or displayed on or stored in Company computers. Employees encountering or receiving this kind of material should report the incident to their supervisors immediately.

***Games and entertainment software.*** Employees may not use the company's Internet connection to download games or other entertainment software, including screen savers, or to play games over the Internet. No employee shall download any software from the Internet without express permission. This includes messaging software such as AOL and MSN, windows skins, music files (*e.g.*, MP3), software updates, or enhancements.

***Illegal copying.*** Employees may not illegally copy material protected under copyright law or make that material available to others for copying. Employees may not agree to a license or download any material for which a registration fee is charged without first obtaining express written permission from the Company.

***Accessing the Internet.*** To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to a Company network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer being used is not connected to the Company's network.

***Virus detection.*** Files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to electronic mail; and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Company's computer network. Employees should never download files from the Internet, accept electronic mail attachments from outsiders, or use disks from non-Company sources without first scanning the material with Company-approved virus-checking software. If

employees suspect that a virus has been introduced into the Company's network, they should notify the Company immediately.

***Sending unsolicited electronic mail (spamming).*** Without the express permission of their supervisors, employees may not send unsolicited electronic mail to persons with whom they do not have a prior relationship.

***Alternating attribution information.*** Employees must not alter the "From:" line or other attribution-of-origin information in electronic mail, messages, or postings. Anonymous or pseudonymous electronic communications are forbidden. Employees must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, making postings to newsgroups, sending electronic mail, or otherwise communicating on-line.

***Use of encryption software.*** Employees may not install or use encryption software on any of the Company's computers without first obtaining written permission from their supervisors. Employees also may not use passwords or encryption keys that are unknown to their supervisors.

***Amendments and revisions.*** This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

***Violations of this policy.*** Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability. If any employee feels that he or she has witnessed or been the subject of conduct in violation of this policy, the employee should utilize the complaint procedure set forth in the Company's EEO policy.

# Court of Appeals

Memorandum

To: All Judges

From: William L. Martin, III

Subject: Committee Assignments

Date: May 29, 2008

Chief Judge Barnes asked that I distribute to you the Committee Assignments which were discussed at the Banc Meeting on Tuesday and which were part of the by-product of our Court Planning Session and Strategic Plan for the Court which came out of our meeting at Brasstown Valley. Chief Judge Barnes Committees are as follows:

**Uniform Practices for Hiring and Retention of Experienced Staff**

Presiding Judge J.D. Smith, Chair
Judge John J. Ellington
Judge Herbert E. Phipps
Staff to Committee: Jan Kelley and Bill Martin

**Better Training for Work Procedures and Policies Practices**

Judge M. Yvette Miller, Chair
Judge A. Harris Adams
Judge Debra Bernes
Staff to Committee: Holly Sparrow, Bill Martin and Jan Kelley

**Legal On-Line Research and Training Program**

Presiding Judge Edward H. Johnson, Chair
Judge Gary B. Andrews
Judge Charles B. Mikell
Judge Debra Bernes
Staff to Committee: John Ruggeri, Holly Sparrow and Jan Kelley

A. Report for Committee on Better Training for Work Procedures

1. Information and recommendation for policies on discrimination and harassment

2. Information and recommendation for policies on prohibited use of technologies

3. Ethics for staff attorneys suggestion to include in IOM

B. Suggestion for a protocol for hiring a judicial office employee already employed in another office.

C. Proposal to assign a floating staff attorney to the chief judge on a continuing basis effective January 1, 2009

## TELEPHONES AND OTHER COURT TECHNOLOGY RESOURCES

### A. Business Use Policy

**The Court provides telephones, electronic mail and other electronic resources to employees to assist them in performing their jobs. The Court therefore, incorporates into this manual the Georgia Technology Authority's policy on use of Information Technology Resources as summarized below. In addition, the Court reserves the right to monitor business-related telephone calls and electronic mail messages conducted in the workplace as well as to retrieve and read any data composed, transmitted or received through online connections and/or stored on Court servers or other Court property.**

### B. Personal Use

**Occasional personal use of the telephone, Internet connectivity and email that do not involve any inappropriate use as described below is permitted by the Court. Any such use should be brief, infrequent and should not interfere with the employee's job performance, duties or responsibilities.** It is preferable that employees make such necessary personal calls or send email messages during their 15 minute breaks, but in no case should personal calls exceed 15 minutes in a day. Violation of this policy will result in disciplinary action. No personal long distance calls shall be made on office telephones unless charged to the employee's personal credit card or home telephone account.

### C. Inappropriate Use

**Inappropriate use of technology resources includes, but is not limited to:**

(1) **Conducting private or personal for-profit activities.**

(2) **Conducting unauthorized not-for-profit business activities.**

(3) **Conducting any illegal activities as defined by Federal, State and local laws or regulations.**

(4) **Creating, accessing or transmitting sexually explicit, obscene or pornographic material.**

(5) **Creating, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing or intimidating.**

(6) **Creating, accessing or participating in online gambling.**

(7) **Infringing of any copyright, trademark, patent or other intellectual property right.**

(8) **Performing any activity that could reduce the security of the system/network, degrade the system/network performance or cause the loss of, corruption of, or prevent full access to data.**

(9) **Attempting to modify or remove computer equipment, software or peripherals without proper authorization.**

(10) **Attempting to libel or otherwise defame any person.**

(11) **Using another employee's access for any reason unless explicitly authorized.**

(12) **Conducting any activity or solicitation for political or religious causes.**

(13) **Distributing State data and information without authorization.**

**An attempt to use technology resources inappropriately will be treated in the same manner as the actual use of the resources inappropriately.**

**Violation of the Court or State policy on the use of technology resources may result in disciplinary action, termination or criminal prosecution.**

D. No Court equipment is to be used for viewing pornographic or salacious material, sending or receiving same, except as may be necessary in the review of issues on appeal.

Clerk's Office Policies

**A. Business Use Policy**

**The Court provides telephones, electronic mail, and other electronic resources to employees to assist them in performing their jobs. The Court therefore, incorporates into this manual the Georgia Technology Authority's policy on use of Information Technology Resources as summarized below. In addition, the Court reserves the right to monitor business-related telephone calls and electronic mail messages conducted in the workplace as well as to retrieve and read any data composed, transmitted or received through online connections and/or stored on Court servers or other Court property.**

**B. Personal Use**

**Occasional personal use of the telephone, Internet connectivity, and email that do not involve any inappropriate use as described below is permitted by the Court. Any such use should be brief, infrequent, and should not interfere with the employee's job performance, duties or responsibilities.** It is preferable that employees make such necessary personal calls or send email messages during their 15 minute breaks, but in no case should personal calls exceed 15 minutes in a day. Violation of this policy will result in disciplinary action. No personal long distance calls shall be made on office telephones unless charged to the employee's personal credit card or home telephone account. ???

**C. Inappropriate Use**

**Inappropriate use of technology resources includes, but is not limited to:**

(1) **Conducting private or personal for-profit activities.**

(2) **Conducting unauthorized not-for-profit business activities.**

(3) **Conducting any illegal activities as defined by federal, state, and local laws or regulations.**

(4) **Creating, accessing or transmitting sexually explicit, obscene, or pornographic material.**

(5) **Creating, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing or intimidating.**

(6) **Creating, accessing or participating in online gambling.**

(7) **Infringing of any copyright, trademark, patent or other intellectual property right.**

(8) **Performing any activity that could reduce the security of the system/network, degrade the system/network performance, or cause the loss of, corruption of, or prevent full access to data.**

(9) **Attempting to modify or remove computer equipment, software or peripherals without proper authorization.**

(10) **Attempting to libel or otherwise defame any person.**

(11) **Using another employee's access for any reason unless explicitly authorized.**

(12) **Conducting any activity or solicitation for political or religious causes.**

(13) **Distributing state data and information without authorization.**

**An attempt to use technology resources inappropriately will be treated in the same manner as the actual use of the resources inappropriately.**

**Violation of the Court or State policy on the use of techonology resources may result in disciplinary action, termination or criminal prosecution.**

# Court of Appeals

## Memorandum

---

**To:** William L. Martin, III

**From:** H. Sparrow

**Subject:** Committee - Better Training for Work Procedure and Policies Practices

**Date:** July 17, 2008

---

Attached you will find the following items for consideration in advance of your meeting with Judge Miller, Chair of the above committee.

(1) Pages 15 and 26 of the Internal Operations Manual. See Paragraph A on Page 15 and Paragraph P on Page 26.

(2) Pages 11-12 and 20 of the Office Policies of the Clerk's Office. See Items B and C on Pages 11-12 and 13 (B) of Page 20.

(3) A copy of the Sexual Harassment Policy prepared by the Supreme Court Committee for Gender Equality in 1995. This is followed by a copy that I revised for your consideration sometime ago.

(4) An equal employment policy prepared for an employment seminar presented by the law firm of Freeman, Mathis and Gary.

(5) Some selected pages from the U.S. EEOC web site.

I have asked Jan Kelley if she has anything at hand she would like to give you. Also, if you want me to contact the Access and Fairness in the Courts Committee (successor to the Committee on Gender Equality) to see if that committee has any more current materials that might be of interest to you, I will do so. Just let me know what you want me to do.

# Court of Appeals

## Memorandum

**To:** Bill Martin

**From:** H. Sparrow

**Subject:** Policies on Use of Technology

**Date:** July 28, 2008

Here are some additional resources on internet use (or technology use) policies that I found in my file after our chat with Judge Miller. The first is from another Freeman, Mathis and Gary mini-seminar and the second is the GTA policy on appropriate use of information technology resources. There are two copies of the GTA policy: (1) the 2008 version from the GTA webpage and (2) the copy that was distributed by Judge Smith when he was the chief in 2003. The inappropriate usage list is basically the same for both copies.

A. Report for Committee on Better Training for Work Procedures

1. Information and recommendation for policies on discrimination and harassment

2. Information and recommendation for policies on prohibited use of technologies

3. Ethics for staff attorneys suggestion to include in IOM

B. Suggestion for a protocol for hiring a judicial office employee already employed in another office.

C. Proposal to assign a floating staff attorney to the chief judge on a continuing basis effective January 1, 2009

# Court of Appeals

## Memorandum

**To:** William L. Martin, III

**From:** H. Sparrow

**Subject:** Committee - Better Training for Work Procedure and Policies Practices

**Date:** July 17, 2008

Attached you will find the following items for consideration in advance of your meeting with Judge Miller, Chair of the above committee.

(1) Pages 15 and 26 of the Internal Operations Manual. See Paragraph A on Page 15 and Paragraph P on Page 26.

(2) Pages 11-12 and 20 of the Office Policies of the Clerk's Office. See Items B and C on Pages 11-12 and 13 (B) of Page 20.

(3) A copy of the Sexual Harassment Policy prepared by the Supreme Court Committee for Gender Equality in 1995. This is followed by a copy that I revised for your consideration sometime ago.

(4) An equal employment policy prepared for an employment seminar presented by the law firm of Freeman, Mathis and Gary.

i) Some selected pages from the U.S. EEOC web site.

I have asked Jan Kelley if she has anything at hand she would like to give you. Also, if you want me to contact the Access and Fairness in the Courts Committee (successor to the Committee on Gender Equality) to see if that committee has any more current materials that might be of interest to you, I will do so. Just let me know what you want me to do.

Employees are responsible for preserving their cards from loss and following the rules of GBA relative to replacement. Even though buildings are protected by security screening measures, employees are responsible for their personal belongings .

Employees must surrender all room keys and security /identification badges immediately upon termination of employment.

**Nepotism, Discrimination or Harassment**

**A. Nepotism**

Any person who is related by blood or marriage to a sitting judge on the Court of Appeals is ineligible for employment by the Court or any of its offices.

The employment of an individual who is a relative of another Court of Appeals employee by blood or marriage shall be discouraged. Such relationship shall not be an automatic barrier to employment, but shall require the approval of the Clerk in each case. Willful and intentional failure to disclose such relationship may be cause for disciplinary action.

These policies shall not apply to any employees and their relatives by blood or marriage who were employed by the court on April 1, 1993.

**B. Equal Opportunity**

It is the policy of the Court of Appeals to provide equal opportunity for employment and the benefits of employment based on performance on a non-discriminatory basis. (IOM, page 17)

**C. Discrimination or Harassment**

Discrimination or harassment based on race, color, religion, sex, age, disability, or national origin will not be tolerated. Sexual harassment, subtle or otherwise, shall not be tolerated. Violators of this harassment policy are subject to disciplinary action including termination and/or referral for criminal prosecution. Malicious or frivolous complaints of sexual harassment shall result in corrective or disciplinary action against the accuser. Voluntary compliance with this harassment policy is an indication of professionalism and will create a healthy environment for all.

Sexual harassment is defined as "any unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct of a sexual nature." It occurs when:

(1) Sexual favors are demanded " as a term or condition of employment." For example, a supervisor demands that a subordinate employee sleep with the supervisor or the subordinate employee will be fired.

(2) Sexual demands, once made, are refused and the employee faces an adverse consequence for that refusal. For example, an employee rejects the sexual advance of the employee's supervisor and is demoted or later fired for the refusal.
(3) The acts of verbal abuse, physical touching, sexual demands or other conduct of a sexual nature are so pervasive and persistent as to have "the effect of unreasonably interfering with an individual's work performance or creating an offensive and intimidating working environment" for an employee. For example, males tease and insult women in the workplace with obscene jokes, sexual innuendoes, or similar conduct which embarrass and offend the female employees.

An employee who believes they have been sexually harassed should attempt to resolve the problem with the person with whom there is a problem. If this is too difficult for the employee or proves ineffective, the victim should contact either the Court Executive or Chief Judge who will investigate the accusation and recommend to the Court the actions necessary to resolve the problem. See COA Sexual Harassment Policy Table

**Political Activity**

Political activity on state time or property is absolutely prohibited and is subject to disciplinary action.

On the other hand, employees have the right to cast their vote, express their opinions, make political contributions and support the candidates of their choice. Employees should be mindful that they work in a government organization, and these activities should be conducted during their off duty hours only. Employees should regulate their activities to minimize the risk of conflict with their court duties and so those activities will not detract from the dignity of their office or the court. (IOM page 19.)

No employee shall be required, coerced, expected, induced or encouraged as a condition of employment in any form whatsoever to make any contribution, loan, subscription, or assessment for any political purpose, and no employee shall use, seek, or promise to use his or her position or influence, directly or indirectly, in connection with the solicitation or receipt of any such contribution, loan, subscription, or assessment.

**Performance Evaluation**

Regular employees' job performance will be evaluated on an annual basis approximately 5 weeks prior to the employee's hiring anniversary date. The overall rating will be determinative of continued employment.

Employees may be hired on a probationary status. Probationary employees will be evaluated 3 months from the hiring anniversary date and again at the end of the fifth month. The overall rating of the second evaluation will be determinative of a recommendation that the employee be retained and changed to the status of a regular employee.

| | | |
|---|---|---|
| (2) Second offense | 10 days suspension w/o pay | Dismissal |
| (3) Third offense | Dismissal | |

12. Loafing

| Offense Number | Minimum | Maximum |
|---|---|---|
| (1) First offense | Written warning | 1 day suspension w/o pay |
| (2) Second offense | 5 days suspension w/o pay | 10 days suspension w/o pay |
| (3) Third offense | 15 days suspension w/o pay | Dismissal |

13. Mistreatment of the Public or Other Employees

A. Verbal Abuse

| Offense Number | Minimum | Maximum |
|---|---|---|
| (1) First offense | Written warning | 1 days suspension w/o pay |
| (2) Second offense | 5 days suspension w/o pay | Dismissal |
| (3) Third offense | 15 days suspension w/o pay | Dismissal |

B. Sexual and Other Harassment

| Offense Number | Minimum | Maximum |
|---|---|---|
| (1) First offense | 5 days suspension w/o pay | Dismissal |
| (2) Second offense | Dismissal | |

C. Sexual involvement or physical abuse.

| First Offense - Dismissal |
|---|

14. Political Activity

IOM

# IX. PERSONNEL

## A. EQUAL OPPORTUNITY

It is the policy of the Court of Appeals of Georgia to provide equal opportunity for employment to all employees and applicants for employment on a non-discriminatory basis. No person shall, on the basis of race, color, religion, national origin, age, sex, or mental or physical handicap be excluded from employment by, participation in, be deprived of, or be subject to discrimination. It is the policy of the Court of Appeals of Georgia to provide equal opportunity for employment, compensation, promotion, training, and other conditions of employment, on the basis of assessed qualifications, responsibility level and demonstrated performance.

## B. SALARIES

1. As determined by the court and legislature. Categories by experience are generally in line with the State Merit System. "Experience" means years since admission to any Bar together with active practice of law and service as staff attorneys of this Court or the Supreme Court. (**Source** of this sentence: Order of 9/30/64, as stated in Minute Book 15, p. 294) One-half of the salaries of the Reporter, Assistant Reporter, Assistant to the Reporter, and Reporter's Clerk, all as set by the Supreme Court, shall be paid by the Court of Appeals.

   The salaries of the staff attorneys and of the Deputy Clerk shall be the same as those respective positions in the Supreme Court insofar as possible. The salaries of Research Associates (summer interns) shall be set by the Court.

2. The following procedure shall be followed for any salary adjustment for Clerk's Office personnel and floating administrative assistants which is not a regular salary scale adjustment, a cost of living increase, merit increase or the like.

   a. The Clerk/Court Administrator shall present the judge in charge of the Clerk's Office with a report stating the requested salary adjustment and the reasons therefore.

   b. The report shall contain a work history and salary history of the employee while at the Court of Appeals.

   c. The Fiscal Officer shall present the Judge in charge of the Clerk's Office with a complete fiscal history of the employee, a complete leave history of the employee and a fiscal note stating whether or not the Court has funds available for any salary increase and from which source or sources those funds are available.

## P. NEW EMPLOYEE ORIENTATION GUIDELINE

The judge hiring the employee, the fiscal officer and/or the clerk/court administrator where appropriate, should direct new employees to the Internal Operations Manual and the Rules of the Court of Appeals for specifics about the court and the court's fiscal policies. Also, new employees should be oriented on the role of the judiciary; the important part each employee plays in fulfilling the court's public service role; the court's chain of command; each person's area of responsibility; and the following:

1. Confidentiality.
2. Office hours.
3. Outside employment and activities, including political involvement.
4. Role of summer research associates.
5. Use of Lexis, Westlaw, Georgia Law on Disc, Shepard's, Shepard's on CD Rom, telephone, copy machine, postage machine, and court stationery.
6. Method for ordering supplies.
7. Handling of transcripts and briefs, e.g., no writing on briefs or transcripts.
8. Judge's preferences as to opinion drafting.
9. No smoking policy.
10. Health, life insurance and retirement benefits.
11. Punctuality, sick leave, vacation, holidays, lunch breaks, absenteeism.
12. Parking arrangements.
13. Space allocation for staff attorneys.
14. Staff attorneys.
15. Continuing legal education.
16. Travel reimbursement.
17. Opinion drafting.
18. Proper attire.

No mention of equal opportunity policies here.

## Q. COURT PARKING POLICY

The Court of Appeals now controls the parking spaces for its employees. All spaces are located in the Judicial-Old Labor, Trinity-Washington and Judicial-Old Labor Courtyard parking. Spaces that once were assigned to individuals by Georgia Building Authority (GBA) are now under the control of the Court.

The following parking facility procedures will be administered by the Chief Judge or his/her designee:

1. All space assignments and records will be maintained by the Court.

2. Those individuals who transferred their parking space from their names to the Court of Appeals have been assured that they can continue to use those spaces originally assigned to them until they

# SEXUAL HARASSMENT POLICY

## A Model for Georgia Courts

Prepared by the
Supreme Court Committee for Gender Equality

(Source: Minutes, June 1995 Banc Meeting)

Appendix 8

# SEXUAL HARASSMENT POLICY
## A Model for Georgia Courts

## TABLE OF CONTENTS

# SEXUAL HARASSMENT

## I. PURPOSE

Court employees are entitled to work in an environment free from sexual harassment. The purpose of this policy is to achieve a workplace free from sexual harassment by establishing a procedure for submitting complaints regarding sexual harassment and for the investigation and resolution of those complaints.

## II. SCOPE

This policy shall apply to all judicial and non–judicial employees. This policy governs the process for the filing, investigation, and resolution of a complaint. The policy does not govern the grievance and appeal procedure. This policy does not govern the discipline procedure.

## III. SEXUAL HARASSMENT DEFINED

Discrimination or harassment based on race, color, religion, sex, age, disability, or national origin will not be tolerated in the courts. Sexual harassment is of particular concern to court management, and any form of sexual harassment will not be permitted. Sexual harassment is defined as "any sexual advances, requests for sexual favors or other verbal or physical conduct of a sexual nature, which is unwelcome." It occurs when:

(1) Sexual favors are demanded "as a term or condition of employment." Example: A supervisor demands sexual favors from a subordinate and threatens with termination.

(2) Sexual demands, once made, are refused and the employee faces an adverse consequence for that refusal. Example: An employee rejects the sexual advance of the supervisor, is demoted and later fired for the refusal.

(3) The acts of verbal abuse, physical touching, sexual demands or other conduct of a sexual nature are so pervasive and persistent as to have "the effect of unreasonably interfering with an individual's work performance or creating an offensive and intimidating working environment" for an employee. Example: Persons tease and insult others in the workplace with obscene jokes, sexual innuendoes or similar conduct designed to embarrass and offend.

Sexual harassment, subtle or otherwise, shall not be tolerated. Voluntary compliance with the policy and procedure outlined below will increase professionalism and create a healthy environment for all. Malicious or frivolous complaints of sexual harassment shall result in corrective or disciplinary action against the accuser.

## IV. POLICY

A. 1. No employee shall engage in conduct constituting sexual harassment. Any employee determined after investigation to have engaged in conduct constituting sexual harassment shall be disciplined.

2. Supervisors who knew or should have known of incidents of sexual harassment and failed to take appropriate action in accordance with this policy shall be disciplined.

3. An employee who takes reprisals against another employee for (1) filing a complaint alleging sexual harassment or (2) for appearing as a witness for any party in a sexual harassment complaint shall be disciplined. An employee who submits a fraudulent or bad faith claim of sexual harassment shall be disciplined.

4. The process for filing complaints and for investigation and resolution of complaints shall be free from bias and intimidation.

5. Conduct occurring off duty or off court premises may constitute sexual harassment.

6. Any judicial or non-judicial employee who has reason to believe that another judicial or non-judicial employee is the victim of sexual harassment should encourage the victim to submit a complaint. In the alternative, the judicial or non-judicial employee may inform a designated person of the existence of a possible complaint.

## V. PROCEDURE

A. Designated Person.

1. The judge of each court shall designate a person on the staff to receive complaints of sexual harassment as well as a person to serve in such position in the event the complaint is against the person designated to hear the complaints. The Executive Director of the Office of Gender Equality, in consultation with the court administrator for each district, shall appoint from among the employees of that district a designated person for each judicial administrative district. The Executive Director, in consultation with the Director of the Administrative Office of the Courts, shall appoint from among the employees of the Administrative Office of the Courts a designated person for that office. The names of the designated persons shall be published as part of the policy of the court, district or office from which designated.

2. The person selected as designated person shall display through interest, education, and experience the ability to mediate and negotiate the settlement of disputes among employees. The duties of the designated person shall be added to the job description of the person selected.

3. The Executive Director, in consultation with the Executive Director of the Institute of Continuing Judicial Education, shall develop a program for the initial and continuing education of designated persons in the skills necessary for the successful resolution of complaints of sexual harassment and in the techniques of witness interviewing.

B. Informal Process for Submitting a Complaint of Sexual Harassment Against a Court Employee

1. An employee who is the victim of sexual harassment should inform the harasser that the behavior is unwelcome or submit a complaint to a designated person.

   a. Submitting the complaint to the designated person for the district in which the victim is employed is preferred. A complaint may be submitted to any other designated person. The designated person for the district shall provide to employees the names, addresses, and telephone numbers of all designated persons.

2. The designated person shall receive and investigate informal complaints of sexual harassment, facilitate communication between the parties, and resolve the complaint.

C. Formal Process for Submitting a Complaint of Sexual Harassment Against a Court Employee

1. A formal complaint shall be written. Upon request the designated person shall assist the complainant in submitting a written complaint. A formal complaint should be submitted if:

   a. the informal process does not resolve the complaint

   b. the complaint is a second complaint against the same harasser after the harasser had been informed that the behavior was unwelcome, whether or not submitted by the same complainant; or

   c. in the discretion of the designated person or the complainant, the conduct complained of is egregious. In determining the seriousness of the conduct the designated person shall consider but is not bound by the request of the complainant.

2. The designated person shall receive formal complaints of sexual harassment and refer them to the designated person of the district of the complainant's employment or the designated person at the Administrative Office of the Courts. If the designated person of the district is the alleged harasser, the designated person shall refer the complaint to the Director of the Administrative Office of the Courts. If the complainant is employed by the Administrative Office of the Courts, the designated person shall refer the formal complaint to the three-member panel appointed by the Judicial Council. Upon referral, the designated person shall provide the alleged harasser with a copy of the written complaint.

3. The designated person of the district shall investigate the complaint and determine whether the conduct complained of occurred and whether the conduct constitutes sexual harassment. The designated person of the district shall prepare a written report of the nature of the investigation and the findings and conclusions of the investigation. The report shall be completed within twenty days of the referral from the designated person. The court administrator shall provide a copy of the report to the parties.

4. The designated person of the district may recuse himself or herself from the investigation and determination if the designated person of the district is the immediate supervisor of either party, is a personal friend or member of the immediate family of either party, is so closely involved in the matter that the impartiality of the investigation or determination may be questioned, or determines that the time required for the investigation and determination is greater than the designated person of the district can provide.

5. If the designated person of the district does not conduct the investigation and determination, the designated person of the district shall refer the matter within three days to a three member panel appointed by the designated person of the district for that purpose. The designated person of the district shall notify all parties of the referral.

6. The panel shall investigate the complaint and determine whether the conduct complained of occurred and whether the conduct constitutes sexual harassment. The panel shall prepare a written report of the nature of the investigation and the findings and conclusions of the investigation. The panel may include in the report a recommendation regarding discipline. The panel shall complete the report within twenty days of the appointment of the panel. The panel shall file the report with the designated person of the district and provide a copy to the parties. Provided, however, that this time period may be extended by the panel for a reasonable time for good cause shown.

7. At the conclusion of the investigation and determination the designated person of the district shall impose discipline in accordance with the applicable local policies and procedures regarding discipline.

8. Either party may submit a grievance regarding the findings of the report by submitting the grievance to the Judicial Council of Georgia. Only the person disciplined may submit a grievance regarding such discipline.

D. Process for Submitting a Complaint of Sexual Harassment Against a Person not Employed by the Courts.

1. The process for submitting a complaint against a person who is not an employee of the courts is the same as the process for a complaint against a judge with the exception that the three judges on the panel be from the same Administrative Judicial District.

2. The designated person and, upon referral, the court administrator shall use all reasonable means to resolve the complaint, including referring the complaint to the employer of the harasser or to the regulatory agency to which the harasser is subject.

E. Informal Process for Submitting a Complaint of Sexual Harassment Against a Judge.

1. An employee who is the victim of sexual harassment should inform the harasser that the behavior is unwelcome or should submit a complaint to a designated person.

   a. Submitting the complaint to the designated person for the circuit in which the victim is employed is preferred. A complaint may be submitted to any other designated person.

2. The designated person shall receive informal complaints of sexual harassment and inform the chief judge of the existence of the complaint. If the chief judge is the alleged harasser or if the alleged harasser is the judge of a single judge circuit, the designated person shall notify the Director of the Administrative Office of the Courts or designee. In conjunction with the chief judge or the administrative judge, the designated person shall facilitate communication between the parties and resolve the complaint.

F. Formal Process for Submitting a Complaint of Sexual Harassment Against a Judge.

1. A formal complaint shall be written. Upon request the designated person shall assist the complainant in submitting a written complaint. A formal complaint should be submitted if:

a. the informal process does not resolve the complaint;

b. the complaint is a second complaint against the same harasser after the harasser had been informed that the behavior was unwelcome, whether or not submitted by the same complainant; or

c. in the discretion of the designated person or the complainant, the conduct complained of is egregious. In determining the seriousness of the conduct the designated person shall consider but is not bound by the request of the complainant.

2. The designated person shall receive formal complaints of sexual harassment and refer them to the chief judge of the circuit of the complainant's employment. If the chief judge is the alleged harasser or if the alleged harasser is the judge of a single judge circuit, the designated person shall notify the Director of the Administrative Office of the Courts or designee. Upon referral, the designated person shall provide the alleged harasser and the court administrator with a copy of the written complaint.

3. The chief judge, the administrative judge, or the Director of the Administrative Office of the Courts shall refer the complaint to the Judicial Council. The Council shall appoint a three member panel to investigate the complaint and determine whether the conduct complained of occurred and whether the conduct constitutes sexual harassment. The panel shall prepare a written report of the nature of the investigation and the findings and conclusions of the investigation. The panel may include in the report a recommendation regarding discipline. The panel shall file the report with the Council within twenty days of the appointment of the panel and shall provide a copy of the report to the parties, the chief judge, and the court administrator. Provided, however, that this time period may be extended by the panel for a reasonable time for good cause.

4. The chief judge or the Director of the Administrative Office of the Courts shall take appropriate disciplinary action against the harasser.

5. The judge may petition to have the complaint reviewed by the Judicial Council. The complainant may petition to have the complaint reviewed by the Judicial Qualifications Commission.

G. The Investigative Process.

1. Informal Process re Sections V.B. and V.E. -- The investigation conducted by the designated person is informal. The principal objective of the designated person is not to determine whether sexual harassment occurred in the past but rather to govern future conduct. The designated person shall first talk separately with the complainant and then with the alleged harasser.

The designated person should not talk with witnesses identified by either party unless necessary. The designated person may talk with the parties jointly.

2. Formal Process re Sections V.C. and V.F. — The investigation by the designated person of the district or the three member panel is formal and shall include an interview of the parties and any witnesses identified by the parties. Other witnesses may be called by the official or body conducting the investigation. In order to provide a recommendation regarding discipline, the official or body shall consider discipline imposed in other cases involving similar circumstances.

H. Investigative Panel

1. The investigative panel selected by the designated person of the district shall consist of three members from among the designated persons. No designated person involved in the complaint under investigation may serve on the panel. No designated person supervised directly or indirectly by the designated person of the district may serve on the panel. The three member panel selected by the Judicial Council shall be chosen from its members and/or staff of the Administrative Office of the Courts. The panel shall not be comprised exclusively of one sex. The members of the panel shall select a chair from among themselves.

I. Records.

1. All written complaints, notices, correspondence, reports, and other documents regarding a formal complaint of sexual harassment shall be maintained in a file by the Executive Director of the Office of Gender Equality. The file shall be considered a private record of personnel matters involving personnel policy and procedures.

2. All records of complaints found to be without merit shall be destroyed. Provided, however, that records of complaints found to be without merit but involving the complainant shall not be destroyed but shall be retained as part of the disciplinary file in that action.

3. Records regarding discipline imposed as a result of a complaint of sexual harassment or violation of this policy shall be retained in the Office of Gender Equality.

Draft Revision

COURT OF APPEALS OF GEORGIA
SEXUAL HARASSMENT POLICY
March 8, 2005

I. PURPOSE

Court employees are entitled to work in an environment free from sexual harassment. The purpose of this policy is to achieve a workplace free from sexual harassment by establishing a procedure for submitting complaints regarding sexual harassment and for the investigation and resolution of those complaints.

II. SCOPE

This policy shall apply to all judicial and non-judicial employees. This policy governs the process for the filing, investigation, and resolution of a complaint. The policy does not govern the grievance and appeal procedure. This policy does not govern the discipline procedure.

III. SEXUAL HARASSMENT DEFINED

Discrimination or harassment based on race, color, religion, sex, age, disability, or national origin will not be tolerated in the courts. Sexual harassment is of particular concern to court management and any form of sexual harassment will not be permitted. Sexual harassment is defined as "any sexual advances, requests for sexual favors or other verbal or physical conduct of a sexual nature, which is unwelcome." It occurs when:

(1) Sexual favors are demanded "as a term or condition of employment." Example: A supervisor demands sexual favors from a subordinate and threatens the subordinate with termination.

(2) Sexual demands, once made, are refused and the employee faces an adverse consequence for that refusal. Example: An employee rejects the sexual advance of the supervisor, is demoted and later fired for the refusal.

(3) The acts of verbal abuse, physical touching, sexual demands or other conduct of a sexual nature are so pervasive and persistent as to have "the effect of unreasonably interfering with an individual's work performance or creating an offensive and intimidating working environment" for an employee. Example: Persons tease and insult others in the workplace with obscene jokes, sexual innuendoes or similar conduct designed to embarrass and offend.

Sexual harassment, subtle or otherwise, shall not be tolerated. Voluntary compliance with the policy and procedure outlined below will increase professionalism and create a healthy environment for all. Malicious or frivolous complaints of sexual harassment shall result in

corrective or disciplinary action against the accuser.

IV. POLICY

~~A. 1.~~ No employee shall engage in conduct constituting sexual harassment. Any employee determined after investigation to have engaged in conduct constituting sexual harassment shall be disciplined.

~~2.~~ Supervisors who knew or should have known of incidents of sexual harassment and failed to take appropriate action in accordance with this policy shall be disciplined.

~~3.~~ An employee who takes reprisals against another employee for (1) filing a complaint alleging sexual harassment or (2) for appearing as a witness for any party in a sexual harassment complaint shall be disciplined. An employee who submits a fraudulent or bad faith claim of sexual harassment shall be disciplined.

~~4.~~ The process for filing complaints and for investigation and resolution of complaints shall be free from bias and intimidation.

~~5.~~ Conduct occurring off duty or off court premises may constitute sexual harassment.

~~6.~~ Any judicial or non-judicial employee who has reason to believe that another judicial or non-judicial employee is the victim of sexual harassment should encourage the victim to submit a complaint. In the alternative, the judicial or non-judicial employee ~~may~~ should inform ~~a~~ the designated person of the existence of a possible complaint.

V. PROCEDURE

A. Designated Person.

1. ~~The judge of each court shall designate a person on the staff to receive complaints of sexual harassment as well as a person to serve in such position in the event the complaint is against the person designated to hear the complaints. The executive Director of the Office of Gender Equality in consultation with the court administrator for each district, shall appoint from among the employees of that district a designated person for each judicial administrative district. The Executive Director, in consultation with the Director of the Administrative Office of the Courts, shall appoint from among the employees of the Administrative Office of the Courts a designated person for that office. The names of the designated persons shall be published as part of the policy of the court, district, or office from which designated.~~ The Court

has designated the Clerk/Court Administrator to receive complaints of sexual harassment. In the event the complaint is against the person designated to hear complaints, the Chief Judge shall serve in the Clerk/Court Administrator's place. The Clerk/Court Administrator will inform the Chief Judge of any informal or formal complaints made against a judge or employee of the Court. If the complaint is made against the Chief Judge, the Clerk/Court Administrator will inform the most senior judge of the court other than the Chief Judge of the complaint.

~~2. The person selected as designated person shall display through interest, education, and experience the ability to mediate and negotiate the settlement of disputes among employees. The duties of the designated person shall be added to the job description of the person selected.~~

2. The Court shall permit the Clerk/Court Administrator to attend from time to time continuing education programs for developing and maintaining the skills necessary for interviewing witnesses and successful resolution of sexual harassment complaints. The Clerk/Court Administrator shall share this information with the appropriate judges of the court.

~~3. The Executive Director, in consultation with the Executive Director of the Institute of Continuing Judicial Education, shall develop a program for the initial and continuing education of designated persons in the skills necessary for the successful resolution of complaints of sexual harrassment and in the techniques of witness interviewing.~~

B. Informal Process for Submitting a Complaint of Sexual Harassment Against a Court Employee or Judge

1. An employee who is the victim of sexual harrassment should inform the harasser that the behavior is unwelcome or submit a complaint to the person designated in A ~~(2)~~ (1) above.
~~a. Submitting the complaint to the designated person for the district in which the victim is employed is preferred. A complaint may be submitted to any other designated person. The designated person for the district shall provide to the employees the names, addresses, and telephone numbers of all designated persons.~~

2. The Clerk/Court Administrator or Chief Judge as appropriate under A (1) above shall investigate an informal complaint of sexual harassment, facilitate communication between the parties, and resolve the complaint.

C. Formal Process for Submitting a Complaint of Sexual Harrassment Against a Court

Employee or Judge

1. A formal complaint shall be written. Upon request, the designated person shall assist the complainant in submitting a written complaint. A formal complaint should be submitted if:

   a. the informal process does not resolve the complaint;

   b. the complaint is a second complaint against the same harasser after the harasser had been informed that the behavior was unwelcome, whether or not submitted by the same complainant; or

   c. in the discretion of the designated person, or the complainant, the conduct complained of is egregious. In determining the seriousness of the conduct the designated person shall consider but is not bound by the request of the complainant.

2. The designated person shall receive formal complaints of sexual harrassment and refer them to the Chief Judge or if the complaint is against the Chief Judge to the most senior judge other than the Chief Judge. ~~designated person of the district of the complainant's employment or the designated person at the Administrative Office of the Courts. If the designated person of the district is the alleged harasser, the designated person shall refer the complaint to the Director of the Administrative Office of the Courts. If the complainant is employed by the Administrative Office of the Courts,~~ The Chief Judge or, if necessary, the most senior judge in conjunction with the Clerk/Court Administrator (unless the Clerk Court Administrator is the alleged harasser), ~~the designated person shall refer the formal complaint to the~~ shall appoint a three member panel to handle the formal complaint. ~~appointed by the Judicial Council. Upon referral, the~~ The designated person shall provide the alleged harasser with a copy of the written complaint.

3. ~~The designated person of the district shall investigate the complaint and determine whether the conduct complained of occurred and whether the conduct constitutes sexual harassment. The designated person of the district shall prepare a written report of the nature of the investigation and the findings and conclusions of the investigation. The report shall be completed within twenty days of the referral from the designated person. The court administrator shall provide a copy of the report to the parties.~~

4. ~~The designated person of the district may recuse himself or herself from the investigation and determination if the designated person of the district is the~~

~~immediate supervisor of either party, is a personal friend or member of the immediate family of either party, is so closely involved in the matter that the impartiality of the investigation or determination may be questioned, or determines that the time required for the investigation and determination is greater than the designated person the district can provide.~~

~~5. If the designated person of the district does not conduct the investigation and determination, the designated person of the district shall refer the matter within three days to a three member panel appointed by the designated person of the district for that purpose. The designated person of the district shalll notify all parties of the referral.~~

~~6.~~ The panel shall investigate the complaint and determine whether the conduct complained of occurred and whether the conduct constitutes sexual harassment. The panel shall prepare a written report of the nature of the investigation and the findings and conclusions of the investigation. The panel shall complete the report within twenty days of the appointment of the panel provided, however, that this time period may be extended by the panel for a reasonable time for good cause shown. The panel shall file the report with the ~~designated person of the district~~ Clerk/Court Administrator and provide a copy to the parties, the Chief Judge and the Court's Personnel Office. ~~Provided, however, that this time period may be extended by the panel for a reasonable time for good cause shown.~~

4. ~~7.~~ At the conclusion of the investigation and determination, the ~~designated person of the district~~ Court may impose discipline in accordance with the applicable ~~local~~ policies and procedures regarding discipline.

~~8. Either party may submit a grievance regarding the findings of the report by submitting the grievance to the Judicial Council of Georgia. Only the person disciplined may submit a grievance regarding such discipline.~~ If the complaint was made against a judge of the Court, the complainant may request the Judicial Qualifications Commission to determine whether there has been a violation of judicial ethics. *(From F. 5.)*

D. Process for Submitting a Complaint of Sexual Harassment Against a Person not Employed by the Courts.

~~1. The process for submitting a complaint against a person who is not an employee of the courts is the same as the process for a complaint against a judge with the exception that the three judges on the panel be from the same Administrative Judicial District.~~ An employee who is the victim of sexual

harrassment should inform the harasser that the behavior is unwelcome or submit a complaint to the person designated in A (1) above. Once a complaint has been submitted to the designated person, he or she shall use all reasonable means to resolve the complaint including communication with the alleged harasser and referring the complaint to the employer of the alleged harasser or to the regulatory agency to which the alleged harasser is subject. (Used parts of A and D 2in this revision)

~~2. The designated person and , upon referral, the court administrator shall use all reasonable means to resolve the complaint, including referring the complaint to the employer of the harasser or to the regulatory agency to which the harasser is subject.~~

F. Delete this whole section on Complaints versus Judge. Now combined into C. See old version for former language of this section.

F. ~~G. The~~ Investigative Process

1. Informal Complaint Process ~~re Sections V. D. and V. E. =~~ The investigation conducted by the designated person is informal. The principal objective of the designated person is not to determine whether sexual harassment occurred in the past but rather to govern future conduct. The designated person shall first talk separately with the complainant and then with the alleged harasser. The designated person should not talk with witnesses identified by either party unless necessary. The designated person may talk with the parties jointly.

2. Formal Complaint Process ~~re Sections V.C. and v. F. =~~ The investigation by the ~~designated person of the district or the~~ three member panel is formal and shall include an interview of the parties and any witnesses identified by the parties. Other witnesses may be called by the ~~official or~~ body conducting the investigation. In order to provide a recommendation regarding discipline, the ~~official or~~ body investigating the complaint shall consider the Court policies on discipline and the discipline imposed in other cases involving similar circumstances.

G. ~~H.~~ Investigative Panel

~~1. The investigative panel selected by the designated person of the district shall consist of three members from among the designated persons. No designated~~ person directly involved in the complaint under investigation may serve on

the panel. ~~No designated person supervised directly or indirectly by the designated person of the district may serve on the panel.~~ ~~The three member panel selected by the Judicial Council shall be chosen from its members and/or staff of the Administrative Office of the Courts.~~ The panel shall not be comprised exclusively of one sex. The members of the panel shall select a chairperson from among themselves.

H. ~~I.~~ Records

1. All written complaints, notices, correspondence, reports, and other documents regarding a formal complaint of sexual harassment shall be maintained in a file by the Court Personnel Office. The file shall be considered a private record of personnel matters involving personnel policy and procedures.

2. All records of informal complaints found to be without merit shall be destroyed. ~~Provided, however, that~~ However, records of complaints found to be without merit ,but in which the complainants have been disciplined ~~involving the complainant shall not be destroyed but~~ shall be retained as part of the complainant's ~~the~~ disciplinary file ~~in that action~~. Records of

~~3. Records regarding discipline imposed as a result of a complaint of sexual harassment or violation of this policy shall be retained in the Office of Gender Equality.~~

Freeman, Mathis and Gary, LLP Presentation

## EQUAL EMPLOYMENT OPPORTUNITY

1. EEO Policy. The Company is committed to maintaining a work environment that is free of inappropriate or unlawful conduct. In keeping with this commitment, we will not tolerate harassment, discrimination or the unlawful treatment of employees by anyone, including any supervisor, co-worker, vendor, client or customer of the Company.

2. Prohibited Conduct. Harassment, discrimination and/or improper conduct consists of misconduct that includes unwelcome conduct, whether verbal, physical, or visual, that is based upon a person's protected status, such as sex, color, race, religion, national origin, age, disability or other protected group status or activity (e.g. opposition to prohibited discrimination or participation in the statutory complaint process) as provided for by law. This includes conduct by someone to another of the same gender. The Company will not tolerate conduct that affects tangible job benefits, that interferes unreasonably with an individual's work performance, or that creates an intimidating, hostile, or offensive working environment. No supervisor or Company employee has authority to engage in such conduct. If you feel you have been subject to the type of conduct prohibited by this policy, you must report this conduct. You are specifically authorized to bypass your supervisor and directly file an EEO complaint with the Human Resources Department as provided for in this policy. If you complain to your supervisor and no action is taken, you are directed to report the conduct as described below to the Human Resources Department. You should report any improper conduct before it becomes severe or pervasive and do not have to wait until it rises to the level of an unlawful action.

3. Sexual Harassment. Sexual harassment deserves special mention. Unwelcome sexual advances, requests for sexual favors, and other physical, verbal, or visual conduct based on sex constitute sexual harassment when (1) submission to the conduct is an explicit or implicit term or condition of employment; (2) submission to or rejection of the conduct is used as the basis for an employment decision; or (3) the conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment. Inappropriate conduct may include explicit sexual propositions, sexual innuendo, suggestive comments, sexually oriented "kidding" or "teasing," "practical jokes," jokes about gender-specific traits, foul or obscene language or gestures, displays of foul or obscene printed or visual material, and physical contact, such as patting, pinching, or brushing against another's body.

4. Complaint Procedure. All employees should help to assure that we avoid any form of unlawful or inappropriate treatment. If you feel that you have experienced or witnessed harassment,

discrimination or unlawful or inappropriate treatment, you are to notify immediately (preferably in writing within 24 hours) the Director of Department of Human Resources. The address and telephone number for the Human Resources Department is _____. If you are not contacted promptly about your complaint, you are to re-file it with the Director of Human Resources and also send a copy by certified mail or contact the Company's Chief Executive Officer at _____. The Company forbids retaliation against anyone who has made a complaint or provides information related to a complaint.

The Company will undertake an objective and appropriate review of any complaint. To the extent practicable and appropriate, the Company will keep any complaint and the terms of its resolution confidential. The Company will take corrective action as it determines is appropriate, including such discipline up to and including immediate termination of employment. The Company will undertake corrective action to stop inappropriate conduct before it rises to the level of an unlawful action. You will be notified as to the outcome of your complaint. If you have any questions about the status of your complaint, you should contact the Director of Human Resources at the above telephone number and address.

The Company recognizes that intentional or malicious false accusations of misconduct can have a serious effect on innocent men and women. Individuals falsely accusing another of misconduct will be disciplined in accordance with the nature and extent of his or her false accusation. The Company encourages any employee to raise questions he or she may have regarding misconduct or this policy with the Director of Human Resources or higher level officer.

Each employee should be aware they have the right to file a charge of discrimination with the Equal Employment Opportunity Commission (EEOC) or other state agency as provided by law. According to the EEOC, the deadline for filing any such charge runs from the last date of unlawful harassment, not from the date that the complaint to the Company is resolved.

I hereby acknowledge that I have received and have reviewed the EEO policy.

_____
Employee Signature

_____
Date

ajs1223

# Court of Appeals

Memorandum

---

**To:** All judges and all court staff

**From:** Chief Judge Smith

**Subject:** State policy on IT resources

**Date:** July 1, 2003

---

The attached memoranda come from Bud Tirey and Technical Support. They remind us of the basic policies and limitations on appropriate use of our court's computers and other information technology resources. As noted, these are the state's minimum policies and limitations. Our court's IT resources are also subject to policies, procedures, and limitations set by the court, particularly with respect to issues affecting confidentiality.

Please advise in writing if you have any questions or any suggestions as to clarification or improvement of court policy in this area.

attachments

**OFFICE OF THE STATE INSPECTOR GENERAL**

**SONNY PERDUE**
Governor

June 27, 2003

**JAMES E. SEHORN**
State Inspector General

**MEMORANDUM**

**TO:** Agency Heads

**FROM:** James E. Sehorn, Georgia State Inspector General

Tom Wade, Acting Executive Director
Georgia Technology Authority

**RE:** State Policy on Appropriate Use of Information Technology Resources

The state of Georgia provides computers and other technology to its employees so they can conduct work-related duties. In turn, employees are responsible for using technology for legitimate work-related purposes. We are asking you to ensure that your agency's employees understand and follow the provisions of the state policy on appropriate use of information technology resources. A copy of the policy is enclosed.

Among the activities prohibited by the policy are:

- business transactions for the personal gain of a state employee;
- activities in violation of federal, state or local laws and regulations;
- creating, accessing or transmitting materials considered sexually explicit or pornographic, discriminatory, offensive, threatening, harassing or intimidating;
- gambling;
- unauthorized distribution of state data and information; and
- compromising the security of an agency's or the state's data network.

Agencies may establish more stringent policies and procedures regarding their employees' use of IT resources, including the Internet and e-mail. Please assist your employees in understanding and complying with the policy. For instance, stress to your employees that when they use any computer at work, they should have no expectation of privacy. These communications are considered to be state property and may be examined by management for any reason including, but not limited to, security and/or employee conduct. In addition, agencies are responsible for preventing improper disclosure of personal information entrusted to them by Georgia residents. Employees should also understand that violating the policy could result in disciplinary actions, including dismissal and criminal prosecution.

The role of the Office of Inspector General includes taking measures to prevent fraud, waste, abuse and corruption. We are bringing the policy on appropriate use of IT resources to your attention at this time as a preventive measure. As leaders of state government, we all must be concerned about preventing the misuse and abuse of the taxpayers' resources. This would certainly include the state's considerable investment in information technology.

We appreciate your assistance in this effort. Feel free to contact us if you have questions or comments.

Enclosure

2 Martin Luther King, Jr. Drive, SW • 1102 West Tower • Atlanta, Georgia 30334
Phone: 404.656.7924 • Toll-Free 866.435.7644 • Fax: 404.657.9716


# Appropriate Use of Information Technology Resources

| POLICY NUMBER: **3.1.3** | EFFECTIVE DATE: 09/10/02 |
|---|---|

## PURPOSE

To establish an enterprise policy regarding appropriate use of State of Georgia information technology (IT) resources.

## SCOPE

All Agencies of the State of Georgia. This policy applies to all employees, contractors, vendors, customers, and others who utilize, possess or have access to State of Georgia IT resources.

## POLICY

***State of Georgia information technology resources are provided to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on Users and is subject to state government policies and applicable state and federal laws. It is the responsibility of Users to ensure that such resources are not misused.***

## STANDARDS

- **To comply with this policy, Users shall refrain from inappropriate use of State of Georgia information technology resources at all times, including during breaks or outside of regular business hours.**

- Inappropriate usage includes (but is not limited to) actual or attempted usage of information technology resources for:

  - Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;

  - Conducting unauthorized not-for-profit business activities;

  - Conducting any illegal activities as defined by federal, state, and local laws or regulations;

  - Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;

- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance;
- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of state data and information;
- Attempts to subvert the security of any state or other network or network resources;
- Use of another employee's access for any reason unless explicitly authorized; or,
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.
- Attempts to libel or otherwise defame any person

- Agencies may establish more stringent policies and procedures consistent with this Enterprise Policy and associated Standards.
- Each Agency reserves the right to retrieve and read any data composed, transmitted or received through online connections and/or stored on their respective servers and /or property. (See enterprise security policy 8.7.3).

**GUIDELINES**

State Agencies provide IT equipment as necessary to employees and others for the efficient and effective performance of their duties. IT equipment is provided to carry out job duties, facilitate business-related research and access to information, and also to enhance communication with customers, vendors, colleagues and others receiving services/products from, doing business with, or seeking information from the State.

Occasional personal use of Internet connectivity and e-mail that do not involve any inappropriate use as described above may occur, if permitted by the Agency. Any such use should be brief, infrequent, and shall not interfere with User's performance, duties and responsibilities.

**AUTHORITY, ENFORCEMENT, EXCEPTIONS** (see Section 1)

- Violations of this Policy and associated Standards may result in disciplinary action, termination, or criminal prosecution.

- Occasional access to information or websites of the Georgia Lottery Corporation shall not constitute nor be considered inappropriate use.

**TERMS AND DEFINITIONS** (see Section 2)

**"Information Technology Resources" or "IT Resources"** means hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

## CONFIDENTIAL COMPANY INFORMATION AND INTERNET, COMPUTER, VOICE AND EMAIL POLICY

***Introduction.*** Certain employees may be provided with access to the Internet to assist them in performing their jobs. The Internet can be a valuable source of information and research. In addition, electronic mail can provide an excellent means of communicating with other employees, customers and clients, outside vendors, and other businesses. Additionally, employees often will be privy to confidential Company information in the course of performing their jobs. Use of all this information, however, must be tempered with common sense and good judgment. Accordingly, the Company has formulated the following guidelines to establish the appropriate parameters for the use of Company property and information. This policy will be administered in conjunction with the Company's EEO policy regarding inappropriate or offensive communications and supersedes any and all prior written policies or verbal authorization granted by any individual within the organization.

***Protecting confidential information.*** Protecting our Company's information is the responsibility of every employee, and we all share a common interest in making sure this information is not improperly or accidentally disclosed. Do not discuss the Company's confidential business with co-workers, unless appropriate, or anyone who does not work for us. Employees may not copy or transmit copyrighted material that is not authorized to be sent, trade secrets of the Company or other entities, or proprietary financial or business operations information of the Company or other entities. Additionally, Company communications and property are confidential. Any employee who accesses another person's computer, voice mail, computer file or data, or property without prior approval by an appropriate officer of the Company will be in violation of this policy.

***Business use.*** Employees should keep personal records and personal business at home. All Company equipment and property, including desks, other physical items, computer systems, computer software, diskettes, electronic mail, and voice mail, should be used appropriately for the business of the Company only. These resources are established, maintained, and

provided by the Company for employees to use for the furtherance of the purpose of the Company and not for personal use.

***Disclaimer of liability for use of the Internet.*** The Company is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk.

***Employee's duty of care.*** Employees should endeavor to make each electronic communication truthful and accurate. Employees should use the same care in drafting electronic mail and other electronic documents as they would for any other written communication. Please keep in mind that anything created or stored on the computer system may be and likely will be reviewed by others.

***Duty not to waste computer resources.*** Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, using Company equipment for outside organizations or commercial ventures, selling Internet or other carrier access time, or otherwise creating unnecessary network traffic. Because audio, video, and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related.

***No expectation of privacy.*** Employees should not have an expectation of privacy or security in electronic communications or anything else they create, store, send, or receive on the computer or telephone system. The computers, computer accounts, and telephones given to employees are to assist them in performance of their jobs. By placing information on the Company's systems, employees grant the Company the right to edit, delete, copy,

republish, and/or distribute such information. In addition, electronic mail may be stored indefinitely on any number of computers, including that of the recipient, and may be sent to nonexistent or incorrect user names may be delivered to persons that you never intended. Copies of these messages may be forwarded to others either electronically or on paper.

***Passwords.*** Passwords are designed to give employees access to all or part of the Company's computer, electronic, and/or telephone systems; they are not designed to guarantee the confidentiality of any message or document. The Company retains the right to enter these systems in its sole discretion.

***Monitoring and accessing employee electronic and telephone transmissions.*** The Company at all times retains the right to access, search, and monitor all directories, indices, diskettes, files, databases, electronic mail messages, voice mail messages, Internet sites visited by employees, chat groups and newsgroups, material downloaded or uploaded by users to the Internet, or any other electronic or telephonic transmissions contained in or used in conjunction with the Company's computer, electronic mail, and voice mail systems and equipment with no prior notice. This right applies both during employees' employment by the Company and after its cessation for any reason or no reason, including whether the cessation is voluntary or involuntary. Additionally, computer, electronic mail, and voice mail messages that have been deleted or erased by employees may remain stored in the Company's computer or telephone system. Accordingly, the Company retains the right to access computer, electronic mail, and voice mail messages for as long as the information may be obtained from any source, even after employee has deleted or erased it.

***Blocking of inappropriate content.*** The company may use software or hardware to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by company networks. In the event employees do encounter inappropriate or sexually explicit material while browsing on the Internet, they should disconnect immediately from the site, regardless of whether the site was subject to Company blocking software.

***Prohibited activities.*** Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, violative of the Company's EEO Policy, or otherwise unlawful or inappropriate may not be sent by electronic mail or other forms of electronic communication (*e.g.*, bulletin board systems, newsgroups, groups, chat groups), downloaded from the Internet, or displayed on or stored in Company computers. Employees encountering or receiving this kind of material should report the incident to their supervisors immediately.

***Games and entertainment software.*** Employees may not use the company's Internet connection to download games or other entertainment software, including screen savers, or to play games over the Internet. No employee shall download any software from the Internet without express permission. This includes messaging software such as AOL and MSN, windows skins, music files (*e.g.*, MP3), software updates, or enhancements.

***Illegal copying.*** Employees may not illegally copy material protected under copyright law or make that material available to others for copying. Employees may not agree to a license or download any material for which a registration fee is charged without first obtaining express written permission from the Company.

***Accessing the Internet.*** To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to a Company network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer being used is not connected to the Company's network.

***Virus detection.*** Files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to electronic mail; and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Company's computer network. Employees should never download files from the Internet, accept electronic mail attachments from outsiders, or use disks from non-Company sources without first scanning the material with Company-approved virus-checking software. If

employees suspect that a virus has been introduced into the Company's network, they should notify the Company immediately.

***Sending unsolicited electronic mail (spamming).*** Without the express permission of their supervisors, employees may not send unsolicited electronic mail to persons with whom they do not have a prior relationship.

***Alternating attribution information.*** Employees must not alter the "From:" line or other attribution-of-origin information in electronic mail, messages, or postings. Anonymous or pseudonymous electronic communications are forbidden. Employees must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, making postings to newsgroups, sending electronic mail, or otherwise communicating on-line.

***Use of encryption software.*** Employees may not install or use encryption software on any of the Company's computers without first obtaining written permission from their supervisors. Employees also may not use passwords or encryption keys that are unknown to their supervisors.

***Amendments and revisions.*** This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

***Violations of this policy.*** Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability. If any employee feels that he or she has witnessed or been the subject of conduct in violation of this policy, the employee should utilize the complaint procedure set forth in the Company's EEO policy.

## CENTRAL STAFF WORKLOAD CALCULATION

**2006 DIRECT APPEALS - TOTAL FILINGS** 3303

TOTAL REVIEWED BY EACH CENTRAL STAFF ATTORNEY

- PER YEAR 551
- PER WEEK 11
- PER DAY 2

**2007 DIRECT APPEALS - TOTAL FILINGS** 3280

TOTAL REVIEWED BY EACH CENTRAL STAFF ATTORNEY

- PER YEAR 547
- PER WEEK 11
- PER DAY 2

*CALCULATIONS BASED ON SIX CENTRAL STAFF POSITIONS.

| | |
|---|---|
| **2006 DIRECT APPEALS** | 2505 |
| Less 22% Dismissed<br>Less 5.9% Withdrawn<br>Less 3 % Transferred | (774) |
| TOTAL | 1731 |
| APPEALS PER JUDGE | 144 |
| APPEALS PER STAFF ATTORNEY - PER YEAR | 48 |
| APPEALS PER STAFF ATTORNEY - PER WEEK (.9246) | 1 |

| | |
|---|---|
| **2007 DIRECT APPEALS** | 2509 |
| Less 21.1% Dismissed<br>Less 5% Withdrawn<br>Less 3.1 % Transferred | (733) |
| TOTAL | 1776 |
| APPEALS PER JUDGE | 148 |
| APPEALS PER STAFF ATTORNEY - PER YEAR | 49 |
| APPEALS PER STAFF ATTORNEY - PER WEEK (.9489) | 1 |

# Court of Appeals

Memorandum

---

**To:** Bill Martin

**From:** H. Sparrow

**Subject:** Policies on Use of Technology

**Date:** July 28, 2008

---

Here are some additional resources on internet use (or technology use) policies that I found in my file after our chat with Judge Miller. The first is from another Freeman, Mathis and Gary mini-seminar and the second is the GTA policy on appropriate use of information technology resources. There are two copies of the GTA policy: (1) the 2008 version from the GTA webpage and (2) the copy that was distributed by Judge Smith when he was the chief in 2003. The inappropriate usage list is basically the same for both copies.

## CONFIDENTIAL COMPANY INFORMATION AND INTERNET, COMPUTER, VOICE AND EMAIL POLICY

***Introduction.*** Certain employees may be provided with access to the Internet to assist them in performing their jobs. The Internet can be a valuable source of information and research. In addition, electronic mail can provide an excellent means of communicating with other employees, customers and clients, outside vendors, and other businesses. Additionally, employees often will be privy to confidential Company information in the course of performing their jobs. Use of all this information, however, must be tempered with common sense and good judgment. Accordingly, the Company has formulated the following guidelines to establish the appropriate parameters for the use of Company property and information. This policy will be administered in conjunction with the Company's EEO policy regarding inappropriate or offensive communications and supersedes any and all prior written policies or verbal authorization granted by any individual within the organization.

***Protecting confidential information.*** Protecting our Company's information is the responsibility of every employee, and we all share a common interest in making sure this information is not improperly or accidentally disclosed. Do not discuss the Company's confidential business with co-workers, unless appropriate, or anyone who does not work for us. Employees may not copy or transmit copyrighted material that is not authorized to be sent, trade secrets of the Company or other entities, or proprietary financial or business operations information of the Company or other entities. Additionally, Company communications and property are confidential. Any employee who accesses another person's computer, voice mail, computer file or data, or property without prior approval by an appropriate officer of the Company will be in violation of this policy.

***Business use.*** Employees should keep personal records and personal business at home. All Company equipment and property, including desks, other physical items, computer systems, computer software, diskettes, electronic mail, and voice mail, should be used appropriately for the business of the Company only. These resources are established, maintained, and

provided by the Company for employees to use for the furtherance of the purpose of the Company and not for personal use.

***Disclaimer of liability for use of the Internet.*** The Company is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Users accessing the Internet do so at their own risk.

***Employee's duty of care.*** Employees should endeavor to make each electronic communication truthful and accurate. Employees should use the same care in drafting electronic mail and other electronic documents as they would for any other written communication. Please keep in mind that anything created or stored on the computer system may be and likely will be reviewed by others.

***Duty not to waste computer resources.*** Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, using Company equipment for outside organizations or commercial ventures, selling Internet or other carrier access time, or otherwise creating unnecessary network traffic. Because audio, video, and picture files require significant storage space, files of this sort may not be downloaded unless they are business-related.

***No expectation of privacy.*** Employees should not have an expectation of privacy or security in electronic communications or anything else they create, store, send, or receive on the computer or telephone system. The computers, computer accounts, and telephones given to employees are to assist them in performance of their jobs. By placing information on the Company's systems, employees grant the Company the right to edit, delete, copy,

republish, and/or distribute such information. In addition, electronic mail may be stored indefinitely on any number of computers, including that of the recipient, and may be sent to nonexistent or incorrect user names may be delivered to persons that you never intended. Copies of these messages may be forwarded to others either electronically or on paper.

***Passwords.*** Passwords are designed to give employees access to all or part of the Company's computer, electronic, and/or telephone systems; they are not designed to guarantee the confidentiality of any message or document. The Company retains the right to enter these systems in its sole discretion.

***Monitoring and accessing employee electronic and telephone transmissions.*** The Company at all times retains the right to access, search, and monitor all directories, indices, diskettes, files, databases, electronic mail messages, voice mail messages, Internet sites visited by employees, chat groups and newsgroups, material downloaded or uploaded by users to the Internet, or any other electronic or telephonic transmissions contained in or used in conjunction with the Company's computer, electronic mail, and voice mail systems and equipment with no prior notice. This right applies both during employees' employment by the Company and after its cessation for any reason or no reason, including whether the cessation is voluntary or involuntary. Additionally, computer, electronic mail, and voice mail messages that have been deleted or erased by employees may remain stored in the Company's computer or telephone system. Accordingly, the Company retains the right to access computer, electronic mail, and voice mail messages for as long as the information may be obtained from any source, even after employee has deleted or erased it.

***Blocking of inappropriate content.*** The company may use software or hardware to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by company networks. In the event employees do encounter inappropriate or sexually explicit material while browsing on the Internet, they should disconnect immediately from the site, regardless of whether the site was subject to Company blocking software.

***Prohibited activities.*** Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, violative of the Company's EEO Policy, or otherwise unlawful or inappropriate may not be sent by electronic mail or other forms of electronic communication (*e.g.*, bulletin board systems, newsgroups, groups, chat groups), downloaded from the Internet, or displayed on or stored in Company computers. Employees encountering or receiving this kind of material should report the incident to their supervisors immediately.

***Games and entertainment software.*** Employees may not use the company's Internet connection to download games or other entertainment software, including screen savers, or to play games over the Internet. No employee shall download any software from the Internet without express permission. This includes messaging software such as AOL and MSN, windows skins, music files (*e.g.*, MP3), software updates, or enhancements.

***Illegal copying.*** Employees may not illegally copy material protected under copyright law or make that material available to others for copying. Employees may not agree to a license or download any material for which a registration fee is charged without first obtaining express written permission from the Company.

***Accessing the Internet.*** To ensure security and avoid the spread of viruses, employees accessing the Internet through a computer attached to a Company network must do so through an approved Internet firewall. Accessing the Internet directly, by modem, is strictly prohibited unless the computer being used is not connected to the Company's network.

***Virus detection.*** Files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to electronic mail; and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Company's computer network. Employees should never download files from the Internet, accept electronic mail attachments from outsiders, or use disks from non-Company sources without first scanning the material with Company-approved virus-checking software. If

employees suspect that a virus has been introduced into the Company's network, they should notify the Company immediately.

***Sending unsolicited electronic mail (spamming).*** Without the express permission of their supervisors, employees may not send unsolicited electronic mail to persons with whom they do not have a prior relationship.

***Alternating attribution information.*** Employees must not alter the "From:" line or other attribution-of-origin information in electronic mail, messages, or postings. Anonymous or pseudonymous electronic communications are forbidden. Employees must identify themselves honestly and accurately when participating in chat groups, making postings to newsgroups, making postings to newsgroups, sending electronic mail, or otherwise communicating on-line.

***Use of encryption software.*** Employees may not install or use encryption software on any of the Company's computers without first obtaining written permission from their supervisors. Employees also may not use passwords or encryption keys that are unknown to their supervisors.

***Amendments and revisions.*** This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

***Violations of this policy.*** Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability. If any employee feels that he or she has witnessed or been the subject of conduct in violation of this policy, the employee should utilize the complaint procedure set forth in the Company's EEO policy.

| GTA | Georgia Technology Authority | |
|---|---|---|
| **Title:** | **Appropriate Use of Information Technology Resources** | |
| **PSG Number:** | P-08-003.01 | **Topical Area:** Security |
| **Document Type:** | Policy | **Pages:** 4 |
| **Issue Date:** | 3/20/08 | **Effective Date:** 3/20/08 |
| **POC for Changes:** | GTA Office of Information Security | |
| **Synopsis:** | Establishes an enterprise policy regarding appropriate use of State of Georgia information technology (IT) resources. | |

## PURPOSE

State of Georgia information technology resources are provided to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on users and is subject to state government policies and applicable state and federal laws. It is the responsibility of Users to ensure that such resources are not misused.

## SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

See Enterprise Information Security Charter (Policy)

## POLICY

State information technology resources are tools to be used to facilitate the execution of official state business. The use of such resources imposes certain responsibilities and obligations on Users and is subject to state government policies and applicable state and federal laws. Users of State information technology resources shall refrain from inappropriate use (as defined in Terms and Definitions) of such resources at all times, including during breaks or outside of regular business hours.

## RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Appropriate Use and Monitoring (Standard)
Electronic Communications Accountability (Standard)
Email Use and Protection (Standard)

## TERMS and DEFINITIONS

**Information Technology Resources or IT Resources** means hardware, software, and communications equipment, including, but not limited to: personal computers, email, internet, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities (including but not limited to: data centers, dedicated training facilities, and switching facilities), and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

**Inappropriate usage** includes (but is not limited to) actual or attempted misuse of information technology resources for:

- Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- Conducting unauthorized not-for-profit business activities;
- Conducting any illegal activities as defined by federal, state, and local laws or
- regulations;
- Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;
- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance;
- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of state data and information;
- Attempts to subvert the security of any state or other network or network
- resources;
- Use of another employee's access for any reason unless explicitly authorized;
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.
- Attempts to libel or otherwise defame any person

# Court of Appeals

Memorandum

---

**To:** All judges and all court staff

**From:** Chief Judge Smith

**Subject:** State policy on IT resources

**Date:** July 1, 2003

---

The attached memoranda come from Bud Tirey and Technical Support. They remind us of the basic policies and limitations on appropriate use of our court's computers and other information technology resources. As noted, these are the state's minimum policies and limitations. Our court's IT resources are also subject to policies, procedures, and limitations set by the court, particularly with respect to issues affecting confidentiality.

Please advise in writing if you have any questions or any suggestions as to clarification or improvement of court policy in this area.

attachments

# OFFICE OF THE STATE INSPECTOR GENERAL

**SONNY PERDUE**
Governor

June 27, 2003

**JAMES E. SEHORN**
State Inspector General

**MEMORANDUM**

**TO:** Agency Heads

**FROM:** James E. Sehorn, Georgia State Inspector General

Tom Wade, Acting Executive Director
Georgia Technology Authority

**RE:** State Policy on Appropriate Use of Information Technology Resources

The state of Georgia provides computers and other technology to its employees so they can conduct work-related duties. In turn, employees are responsible for using technology for legitimate work-related purposes. We are asking you to ensure that your agency's employees understand and follow the provisions of the state policy on appropriate use of information technology resources. A copy of the policy is enclosed.

Among the activities prohibited by the policy are:

- business transactions for the personal gain of a state employee;
- activities in violation of federal, state or local laws and regulations;
- creating, accessing or transmitting materials considered sexually explicit or pornographic, discriminatory, offensive, threatening, harassing or intimidating;
- gambling;
- unauthorized distribution of state data and information; and
- compromising the security of an agency's or the state's data network.

Agencies may establish more stringent policies and procedures regarding their employees' use of IT resources, including the Internet and e-mail. Please assist your employees in understanding and complying with the policy. For instance, stress to your employees that when they use any computer at work, they should have no expectation of privacy. These communications are considered to be state property and may be examined by management for any reason including, but not limited to, security and/or employee conduct. In addition, agencies are responsible for preventing improper disclosure of personal information entrusted to them by Georgia residents. Employees should also understand that violating the policy could result in disciplinary actions, including dismissal and criminal prosecution.

The role of the Office of Inspector General includes taking measures to prevent fraud, waste, abuse and corruption. We are bringing the policy on appropriate use of IT resources to your attention at this time as a preventive measure. As leaders of state government, we all must be concerned about preventing the misuse and abuse of the taxpayers' resources. This would certainly include the state's considerable investment in information technology.

We appreciate your assistance in this effort. Feel free to contact us if you have questions or comments.

Enclosure

2 Martin Luther King, Jr. Drive, SW • 1102 West Tower • Atlanta, Georgia 30334
Phone: 404.656.7924 • Toll-Free 866.435.7644 • Fax: 404.657.9716


# Appropriate Use of Information Technology Resources

| POLICY NUMBER: 3.1.3 | EFFECTIVE DATE: 09/10/02 |
|---|---|

## PURPOSE

To establish an enterprise policy regarding appropriate use of State of Georgia information technology (IT) resources.

## SCOPE

All Agencies of the State of Georgia. This policy applies to all employees, contractors, vendors, customers, and others who utilize, possess or have access to State of Georgia IT resources.

## POLICY

***State of Georgia information technology resources are provided to authorized Users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain responsibilities and obligations on Users and is subject to state government policies and applicable state and federal laws. It is the responsibility of Users to ensure that such resources are not misused.***

## STANDARDS

- **To comply with this policy, Users shall refrain from inappropriate use of State of Georgia information technology resources at all times, including during breaks or outside of regular business hours.**

- Inappropriate usage includes (but is not limited to) actual or attempted usage of information technology resources for:

  - Conducting private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;

  - Conducting unauthorized not-for-profit business activities;

  - Conducting any illegal activities as defined by federal, state, and local laws or regulations;

  - Creation, accessing or transmitting sexually explicit, obscene, or pornographic material;

- Creation, accessing or transmitting material that could be considered discriminatory, offensive, threatening, harassing, or intimidating;
- Creation, accessing, or participation in online gambling;
- Infringement of any copyright, trademark, patent or other intellectual property rights;
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance;
- Conducting any activity or solicitation for political or religious causes;
- Unauthorized distribution of state data and information;
- Attempts to subvert the security of any state or other network or network resources;
- Use of another employee's access for any reason unless explicitly authorized; or,
- Attempts to modify or remove computer equipment, software, or peripherals without proper authorization.
- Attempts to libel or otherwise defame any person

- Agencies may establish more stringent policies and procedures consistent with this Enterprise Policy and associated Standards.
- Each Agency reserves the right to retrieve and read any data composed, transmitted or received through online connections and/or stored on their respective servers and /or property. (See enterprise security policy 8.7.3).

## GUIDELINES

State Agencies provide IT equipment as necessary to employees and others for the efficient and effective performance of their duties. IT equipment is provided to carry out job duties, facilitate business-related research and access to information, and also to enhance communication with customers, vendors, colleagues and others receiving services/products from, doing business with, or seeking information from the State.

Occasional personal use of Internet connectivity and e-mail that do not involve any inappropriate use as described above may occur, if permitted by the Agency. Any such use should be brief, infrequent, and shall not interfere with User's performance, duties and responsibilities.

## AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

- Violations of this Policy and associated Standards may result in disciplinary action, termination, or criminal prosecution.

- Occasional access to information or websites of the Georgia Lottery Corporation shall not constitute nor be considered inappropriate use.

TERMS AND DEFINITIONS (see Section 2)

**"Information Technology Resources" or "IT Resources"** means hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.