GENERAL ORDER 10-9

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS

GENERAL ORDER ADOPTING AUTOMATION SYSTEMS AND SERVICES ACCEPTABLE USE AND SOCIAL MEDIA POLICY

The attached "Automation Systems and Services Acceptable Use and Social Media Policy" is hereby ADOPTED.

Signed this 30 day of August, 2010.

FOR THE COURT:

DAVID FOLSOM
Chief Judge

United States District Court
Eastern District of Texas

AUTOMATION SYSTEMS AND SERVICES ACCEPTABLE USE AND SOCIAL MEDIA POLICY

Adopted: August 2010

Overview

The United States District Court for the Eastern District of Texas has published this Acceptable Use and Social Media Policy to provide guidelines that are consistent with this court's established culture of openness, trust, and integrity. The court is committed to protecting its employees and the judiciary from illegal or damaging actions by computer users.

Purpose

The goal of this policy is to outline appropriate and inappropriate use of the automation systems and services provided to personnel by this court. Automation systems and services include, but are not limited to, Internet services, desktop computers, laptop computers, local and wide area network systems, wireless networking systems, mobile technology devices (i.e., aircards, iPhones, and standard cell phones), telephone systems, audio/video display and conferencing components, e-mail systems, and all custom developed and third-party software applications. Use of these services is subject to the following conditions and compliance with federal judicial conference policy.

Scope

This policy applies to all court employees, with such exemptions as may be authorized by a judge or clerk of court, and apply to others who are provided access to the court's computing resources for the conduct of official government business. These guidelines are not exhaustive. Where no policy or guideline exists, employees should use good judgment and take the most prudent action possible. Employees should consult with their supervisor if uncertain.

Appropriate Use

Employees are encouraged to use the automation systems and services to further the goals and objectives of the district court. The types of activities that are encouraged include:

1. Communicating with fellow employees, lawyers, vendors, and other stakeholders within the context of an individual's assigned responsibilities;

2. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities; and

3. Participating in educational or professional development activities.

Inappropriate Use

Individual use of any of the automation systems and services shall not interfere with another employee's productive use of those same resources. A user shall not violate the policies of any automation systems or services accessed through his or her account. Use of the automation systems and services shall comply with all federal laws and all district court policies and contracts. This includes, but is not limited to, the following:

1. Only computers owned by the court shall be within the court environs. Personally owned PC equipment may not be used.

2. Only software owned and/or approved by the court is authorized for installation on court-owned PCs. Personally owned software may not be installed under any circumstances.

3. All authorized software is to be installed and maintained by systems personnel. Changes and deletions to system files are allowed only by systems personnel.

4. No software games are to be installed or used.

5. All software license agreements are to be honored. When individual copies of software are required, a separate copy of the software must be purchased for each PC using the software. The software may not be used on multiple machines. All software will be installed by systems personnel, and software disks will be kept in the systems area.

6. Non-court personnel are to be kept out of areas where PCs are used. Under no circumstances shall they be allowed to use the equipment.

8. Automation systems or services may not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).

9. Automation systems or services may not be used in any way that violates district court policies or rules, including, but not limited to, the personal use of government office equipment or the Judicial Code of Ethics. The Federal Judiciary allows limited use of government office equipment for personal needs if such use does not interfere with official business and involves minimal additional expense to the government. The limited personal use of government office equipment should only occur during an employee's non-work time. This privilege may be revoked or limited at any time by appropriate district court officials. The district court prohibits use for mass unsolicited mailings, access for non-employees to district court resources or network facilities, uploading and downloading of files for personal use, access to pornographic or gaming sites, and the dissemination of chain letters.

10. Individuals may not establish district court computers as participants in any peer-to-peer network, unless approved by management. Peer-to-peer networking consists of using your computer to store various files (e.g., music, videos, pictures, etc.) and then using the peer-to-peer networking software to make those files available for remote access (typically over the Internet) and/or download by any other person participating in the same peer-to-peer network. Additionally, district court computers may not be used to attach to any other remote computers in a peer-to-peer network for the purpose of accessing or downloading files those computers may be sharing.

11. Individuals may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to the district court without authorized permission.

12. In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments or video files not needed for business purposes.

13. Individuals will only use district court approved services, specifically video conferencing, for voice communication over the Internet.

Security

Access to automation systems and services is controlled by account credentials (*i.e.*, user ID, password, pin number, etc.) supplied by the district court. Each employee is required to read and sign this policy before receiving credentials to access any of the automation systems and services. Users may not share account or password information with another person. Automation systems and services accounts are to be used only by the assigned user of the account for authorized purposes. Attempting to obtain another user's account password is strictly prohibited. A user must contact the IT department to obtain a password reset if he or she has reason to believe that any unauthorized person has learned his or her password.

Networked computer systems include numerous points where unauthorized users can access the network and compromise network security. Users must take all necessary precautions to prevent unauthorized access to the automation systems and services. Precautions include, but are not limited to:

1. Avoid leaving logged-in work stations unattended.

2. Visitors should not be left unsupervised where access to sensitive information is possible.

3. Do not install unauthorized software from Internet downloads, e-mail, attachments, or CD installations. Never click on the "You are a winner!" Internet pop-up window.

4. Passwords should be committed to memory. Do not hide password lists under your keyboard or in the top drawer of your desk.

5. Properly password protect your laptop, iPhone, or Blackberry in case of theft.

6. Properly protect your home PC from viruses and unauthorized personnel if you telecommute.

7. Do not use the "Remember Password" function offered by applications.

Access to the Internet is provided through the Judiciary's Data Communication Network (DCN). As part of the security system of the DCN's Internet gateway, a log is kept of all Internet activity passing through the DCN. The director of information technology or his designee may, with authorization from a judge or clerk of court, monitor automation related activity occurring on district court automation and office equipment or accounts. If activities which do not comply with applicable law or departmental policy are discovered, records retrieved may be used to document activity in accordance with due process.

A log of serial numbers will be maintained by systems personnel for all IT equipment. Court personnel must sign for all portable IT equipment assigned to them, e.g., cell phones, laptop computers.

Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use of the automation systems and services may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all automation and networking resources and facilities;

2. Disciplinary action according to applicable policies; and/or

3. Legal action according to applicable laws and contractual agreements.

Social Media

1. USE OF SOCIAL MEDIA

Social media, professional networking sites, rapid-fire communications, blog sites, and personal websites are all widespread, relatively new, communication technologies. The rules for use of this social media with respect to court employment, however, are identical to the rules for use of other communication methods (such as writing or publishing, telephoning, or even conversation).

Many users of social media identify their employer or occupation. An employee clearly identifies association with the court by using the employee's court e-mail address to engage in social media or professional social networking activity. As stated in Section 5, the use of the employee's court e-mail address to engage in social media or professional social networking activity is prohibited.

Employees must use good judgment and careful discretion about the material or information posted online.

2. PRINCIPLES

The court's reputation for impartiality and objectivity is crucial. The public must be able to trust the integrity of the court. The public needs to be confident that the outside activities of our employees do not undermine the court's impartiality or reputation and that the manner in which the court's business is conducted is not influenced by any commercial, political, or personal interests.

Do not identify yourself as a court employee. By identifying oneself as a court employee, a social networker becomes, to some extent, a representative of the court, and everything he/she posts has the potential to reflect upon the court and its image. It is acknowledged that without identifying oneself as a court employee, an employee may intentionally or unintentionally reveal information that will allow the inference of court employment. If this occurs, the employee assumes the responsibility for representing the court in a professional manner.

3. RESPONSIBILITY

Any material, including photographs, presented online on a court employee website, social media, or e-mail or blog, that pertains to the court by any poster is the responsibility of the court employee, even if court employment can only be indirectly inferred or deduced. Personal blogs should not identify court employment even indirectly; if possible, use your first name only. Do not reference or cite other court employees without their express consent, and even then, do not identify them as court employees.

4. RELEVANT TECHNOLOGIES

This policy includes, but is not limited to, the following specific technologies:

- Classmates
- Digg
- Facebook
- Flickr
- LinkedIn
- LiveJournal
- MySpace
- Personal Blogs
- Personal Websites
- Twitter
- Yahoo! Groups
- YouTube

5. RULES

• Use of the court e-mail address for social networking (e.g., blogs, Facebook, Twitter) is not permitted. Use of an employee's court e-mail address is subject to the same appropriate use policies pertaining to the use of the telephone, namely, limited personal use not interfering with the performance of work responsibilities. E-mail addresses should not be used for "chain" correspondence, solicitation of donations, transmittal of large audio, video, or other files, or any business enterprise.

• Do not identify yourself as a court employee at all in social media. While you can control what you post, you cannot predict nor control what others, even family members or friends, might post on your page or in a blog. Their actions, while harmless in intent, could end up embarrassing you, the court, or worse yet, put you in some danger.

• Maintain professionalism, honesty, and respect. Consider your online dialogue as subject to the same bounds of civility required at work. Employees must comply with laws covering libel and defamation of character. Even non-court specific behavior could have ramifications on your employment status (e.g., photographs in compromising or illegal situations).

• Do not discuss your job responsibilities for the court on the Internet. Be careful to avoid leaking confidential information. Avoid negative commentary regarding the court. Any commentary you post that could reveal an association with the court must contain an explicit disclaimer that states: "These are my personal views and not those of my employer." Again, remember that even harmless remarks could be misconstrued by litigants unfamiliar with court processes (such as *pro se* litigants).

• Observe security protocol. Employees must take care to avoid doing things that would compromise the security of the courthouse and personnel. To maintain security do not post pictures of the courthouse, inside or outside; do not post pictures of court events; and do not post pictures of the court's judicial officers.

• Regularly screen the social media or websites in which you participate to ensure nothing is posted that is contrary to the best interests of the court. Should such items appear, it is your responsibility to contact your supervisor and then immediately delete the communication or information, even closing down your Facebook page, etc., as necessary.

• If any employee becomes aware of social networking activity of other staff that would be deemed distasteful or fail the good judgment test, please contact your supervisor.

6. PRODUCTIVITY IMPACT

The use of court assets (*i.e.*, computers, Internet access, e-mail, etc.) is intended for purposes relevant to the responsibilities assigned to each employee. Social networking sites are not deemed a requirement for any position. Social media activities should not interfere with work commitments.

7. COPYRIGHT

Employees must comply with all copyright laws and reference or cite sources appropriately. Plagiarism applies online as well.

8. TERMS OF SERVICE

Most social networking sites require that users, when they sign up, agree to abide by a Terms of Service document. Court employees are responsible for reading, knowing, and complying with the terms of service of the sites they use. It is not the policy of the court to require employees to use pseudonyms when signing up for social networking sites; however, for some employees in sensitive positions, this might be wise. Employees should check with the Information Technology Department regarding any questions about Terms of Service agreements when accessing the Internet at work.

9. OFF LIMITS MATERIAL

This policy sets forth the following items which are deemed off-limits for social networking whether used at court or after work on personal computers, irrespective of whether court employment is identified:

• Seal and Logos
The district court seal and logos may not be used in any manner.

• Politically Sensitive Areas
Employees may not be seen to support any political party or cause. Employees should never indicate a political allegiance on social networking sites, either through profile information or through joining political groups. Employees should not express views for or against any policy which is a matter of current party political debate. Employees should not advocate any particular position on an issue of current public controversy or debate. If an employee is in doubt, he/she should refer immediately to his/her supervisor or manager.

Canon 5 of the Code of Conduct for Judicial Employees prohibits all active engagement in partisan political activities, including, but not limited to, public endorsement of a candidate or contribution to a political campaign. The Code of Conduct should be consulted for a thorough understanding of the specific prohibitions on political activity contained in Canon 5. In addition, Advisory Opinion No. 92 provides guidelines for political activities.

• Confidential Information
One of the most important obligations of employees is to ensure that non-public information learned in the course of employment is kept confidential. Confidential information is strictly forbidden from any discourse outside of the appropriate employees of the court. Information published on blog(s) must comply with the court's confidentiality policies. This also applies to comments posted on other blogs, forums, and social networking sites. Confidential information is not to be discussed or referred to on such sites, even in private messages between site members who have authorized access to the information. Court employees should also refrain from discussing any of the court's internal processes and procedures, whether they are of a non-confidential or confidential nature.

• Online Recommendations
Some sites, such as LinkedIn, allow members to "recommend" current or former co-workers. If an employee does this as a representative of the court, it may give the appearance that the court endorses the individual being recommended. This could create a liability situation if another entity hires the recommended person on the basis of the recommendation. Accordingly, the court forbids employees to participate in employee recommendations for reasons of liability. All communication of this type should be referred to Human Resources for verification.

10. MONITORING EMPLOYEES' USE OF SOCIAL MEDIA

The court reserves the right to visit and monitor social media sites to ensure that employees are not violating our court's social media policy via court or any other computers, including employees' own personal computers.

11. DISCIPLINARY ACTION

Employees who participate in online communication deemed not to be in the best interest of the court may be subject to disciplinary action. Inappropriate communication can include, but is not limited to:

- Confidential court information or data leakage.
- Inaccurate, distasteful, or defamatory commentary about the court.
- Behavior or communication encouraging behavior that is illegal, grossly unprofessional, or in bad taste.

Disciplinary action can include termination or other intervention deemed appropriate by the court.

12. COURT REPORTER EXCEPTION

Official court reporters have an authorized business reason to establish and maintain websites that identify the court as their place of employment.

Internet Disclaimer

The United States District Court assumes no liability for any direct or indirect damages arising from the use of any district court automation systems or services. It is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its own automation systems. Users are solely responsible for any material accessed and disseminated through the Internet.

Employees are encouraged to use automation systems and services responsibly. Any questions regarding this acceptable use policy should be directed to Smith Wimberley, IT Systems Manager, at (903) 590-1023.

Automation Systems and Services
Acceptable Use Policy User Agreement

I hereby acknowledge that I have read and understand the Automation Systems and Services Acceptable Use Policy of the United States District Court for the Eastern District of Texas. I agree to abide by these policies and ensure that persons working under my supervision abide by these policies. I understand that if I violate such rules I may face legal or disciplinary action according to applicable law or departmental policy.

Name (printed): _____

Signature : _____

Date : _____