SAMPLE POLICY ON USE OF UNOFFICIAL EMAIL ACCOUNTS

Public officials and employees should not use their personal email accounts for work related communications. If an official or employee uses a personal email account for work-related communication (either inadvertently or when it is unavoidable), he or she must ensure that a copy of such email is maintained in official files. This may include, for example, forwarding a copy of each such email immediately to the official's or employee's government email account. This policy applies to all work-related emails sent or received on private accounts, including receipt of unsolicited work-related emails.

With regard to trustees or other purely legislative officials (that is, officials who have no executive branch or administrative roles), personal accounts may be used, but all emails discussing public business that are either sent or received during a public meeting or that include a majority of a quorum of the legislative body, shall also copy an official email account designated by the public body for the purposes of collective and retaining such emails. Moreover, case should be taken that said communications do not violate the Open Meetings Act.

CHAPTER 2 – FILES AND DOCUMENT MANAGEMENT

The IT Bureau provides several drive locations for employees to prepare and store their electronic files. The IT Bureau will work with each Bureau Chief to ensure that files are protected and stored in a secure location. Any files that need to be permanently removed from the network will be removed in accordance with the retention policy identified for each bureau and with the approval of the Bureau Chief/Division Chief.

10.2.1 ARCHIVAL

All OAG email, including inbox and sent box messages, is archived in accordance with archival parameters of the Office's Storage Area Network (SAN) system.

10.2.2 DATA BACKUPS/RESTORATION

Daily differential back up of the OAG network is performed every evening, Monday through Thursday. Weekly and monthly backups are performed as well.

10.2.3 DELETION

The user may delete any data files and/or processing documents that are not subject to retention requirements pursuant to the State Records Act or other applicable laws and regulations. Employees may also request IT assistance for deletion by completing a Request for File Management form.

CHAPTER 6 – INTERNET/E-MAIL ACCESS

10.6.1 GENERAL POLICY – INTERNET AND E-MAIL ACCESS REQUEST/APPROVAL

The Bureau of Information Technology maintains an electronic-mail (e-mail) system and Internet access to conduct business on behalf of the Attorney General's Office. This system, including the equipment and the date stored on the equipment, is at all times, the property of the Illinois Attorney General.

Access to and from the internet and through the office's e-mail system represents potentially significant security exposure for the OAG network.

OAG employees who access the Internet or the Office e-mail system may not use OAG facilities or network connections to make unauthorized connections to, break into, or adversely affect the performance of other computer systems on the network. Access to other computer systems via the Internet does not convey the right to use or connect to these computer systems.

10.6.2 PRIVACY

The Bureau of Information Technology cannot guarantee the privacy of electronic communications because electronic communications are private by nature, and are inherently insecure. Even though passwords appear to provide confidentiality, privacy of messages cannot be assumed. This means that e-mail and Internet transmissions can be read, altered, or deleted by unknown parties without the knowledge or permission of the user who composed, sent or received the message or its attachment(s). In addition, even when e-mail messages or Internet files are deleted or erased, it is still possible to recreate the original message or file. Employees should have no expectation of privacy when using e-mail systems or the Internet.

10.6.3 GUIDELINES ON EMPLOYEE USE

Like all communications conducted on behalf of the Illinois Attorney General, employees must use good judgment in Internet and e-mail use. Each use of the Internet and each e-mail must be able to withstand public scrutiny without adversely affecting the Illinois Attorney General's Office.
OAG employees are responsible for any and all activity initiated by their e-mail ID, user id or personal workstation.

OAG employees may not disclose work related information via the Internet or e-mail system that may adversely affect the public's confidence in the integrity of the office.

Prohibition on Use of Personal E-Mail for Work-Related Business: Employees should not use their personal e-mail accounts for work-related communications. Such work-related communications would constitute public records subject to state records laws. If an employee has an occasion to use his or her personal e-mail for work-related communication (either inadvertently or when it is unavoidable, such as when an employee is sending an email from outside the office and is unable to access the office e-mail system), he or she must ensure that a copy of any work-related e-mail sent or received through a personal e-mail account is maintained in the office files.

CHAPTER 7 – Use of Text Messaging

10.7.1 Guidelines on Employee Use of Text Messaging

Prohibition on Use of Text Messaging for Work-Related Business: Employees should not use text messaging for work-related communications. Such work-related communications would constitute public records subject to state records laws. If an employee has an occasion to use text messaging for work-related communication (either inadvertently or when it is unavoidable, such as when an employee sends a text message because the office e-mail system is not accessible and the recipient cannot be reached via phone call), he or she must ensure that a copy of any work-related text message sent or received by the employee is maintained in the office files.