 <b>User Guidelines for E-mail Communications</b>	Guidelines No.	ITS-1000-G	Rev:	B
	Owner:	IT Security and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
Page 1 of 3				

## 1 Purpose

These guidelines are intended to help students, faculty, and staff maintain the University's accepted standard of e-mail use. In general, any communication from a Cal State L.A. e-mail account is reflective of the University and should therefore be written in an appropriate, ethical, professional, and lawful manner. Inappropriate use of University e-mail accounts, such as sending offensive, abusive, and/or harassing messages, may result in disciplinary action, including any legal action as required by California State Law. Using a University email account indicates that you have read and will abide by these user guidelines.

## 2 Definitions

This section is not applicable to these guidelines.

## 3 Related Documents


The following documents, forms, and logs of the latest issue in effect shall apply to the extent specified herein.

ID/Control #	Title
ITS-8808	Network/E-mail Account Request
ITS-8818	Department E-mail Account Request
ITS-8813	Student NIS Account Application
N/A	California Government Code § 8314
N/A	California Penal Code § 502 and 502.01

## 4 Guidelines

### 4.1 Proper Usage

- a) Any e-mail message containing obscenities, verbal harassment, threats, slander, or offensive comments regarding gender, race, religion, or sexual orientation, or any other inappropriate or unlawful content may not be sent. Violation of this or any guideline herein may result in disciplinary and/or legal action as well as the revocation of the e-mail account and other University computing resource privileges.
- b) Cal State L.A. e-mail accounts should be used only for legitimate University-related purposes.
- c) Do not retrieve or read any other e-mail messages but your own, and do not pose as someone else when sending any e-mail message. Invasion of privacy, unlawful access to


 <b>User Guidelines for E-mail Communications</b>	Guidelines No.	ITS-1000-G	Rev:	B
	Owner:	IT Security and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
	Page 2 of 3			

confidential information, and posing as another person are actions subject to discipline and/or legal action.

- d) Treat your e-mail as a form of permanent correspondence that leaves a permanent record once sent and cannot be recalled.
- e) Never send chain letters via e-mail.
- f) Respect other people's time -- send e-mail only when it needs to be sent. Do not waste your colleagues' time by copying them on messages that don't affect them.
- g) Respect copyrighted material. Do not reproduce and send any material unless all references, quotes, and sources are properly cited.
- h) Do not make changes to someone else's message and pass it on without clearly indicating where changes were made and by whom. Unidentified changes to another's messages constitute misrepresentation.
- i) Since body language cues and verbal intonation are absent from written messages, take care in achieve the proper tone when using e-mail. Sarcasm and humor can be misinterpreted easily.
- j) Do not send "spam" (unwanted junk or mass e-mail).
- k) Before sending campus-wide e-mails, consider whether every person on campus needs to view the message. In cases where it is necessary to send campus-wide e-mails, the sender can create segmented distribution lists that allow the message to be sent gradually throughout the day. Recipients can then access the message over time and not impact instructional programs and network traffic.

## 4.2 Privacy and Monitoring

- a) Mandatory disclosure of the contents of e-mail communications is a possibility. For instance, e-mail communications may be subject to production to people other than the intended recipients pursuant to a Public Records Act request, and to discovery in civil litigation when relevant.
- b) E-mail messages are not private. Once the message has been sent, the sender should have no expectations of privacy regarding it. The message can be forwarded to others, or printed and given to others.
- c) You should assume that e-mail on the Internet is not secure. Unless encrypted, never e-mail any confidential information.
- d) Deleted e-mail communications can be retrieved from the University's archival file backups.
- e) Protect entry to your e-mail account and messages by securing your password. Do not share your password with anyone. If someone else gains access to your password, change it immediately.

 <b>User Guidelines for E-mail Communications</b>	Guidelines No.	ITS-1000-G	Rev:	B
	Owner:	IT Security and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
Page 3 of 3				

- f) University e-mail accounts are subject to internal monitoring if suspicion arises that its usage violates University policy. E-mail messages may be subject to subpoena.

### 4.3 Receiving and Replying to E-mail Messages

- a) Do not assume the validity of a received message.
- b) Read your e-mail regularly. The immediacy of e-mail may be lost if it sits unnoticed in your mailbox for long periods.
- c) Be courteous; reply to e-mail messages within 24 hours, even if it's to let the sender know you will send a lengthier response at another time.
- d) Use the automatic reply feature in Outlook when you will be unable to open e-mail messages for a period of time. You can advise senders of your return date and any other pertinent information that may be helpful in your absence.
- e) Use tracking options in Outlook if you need verification that a message has been delivered and/or read.
- f) Do not use unnecessary space on the e-mail server by keeping outdated and/or unneeded messages. Save them to a local disk if desired.

## 5 Terms, Conditions, and/or Sanctions

All University employees are subject to California Government Code section 8314, which addresses the use of public resources for unauthorized purposes, and California Penal Code sections 502 and 502.01, which deal with unauthorized access to computers, computer systems, computer data, and the criminal penalties that apply.

## 6 Contacts

Questions regarding these guidelines should be directed to [itsecurity@calstatela.edu](mailto:itsecurity@calstatela.edu).