 User Guidelines for Outlook™ Public Folders	Guidelines No.	ITS-1002-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
Page 1 of 6				

1 Purpose

These guidelines establish the University's acceptable standards for using the Microsoft Outlook™ and Outlook™ Web Access (OWA) Public Folders ("Public Folder(s) herein) functionality and help faculty, staff, and departments meet them. Public Folders are a University resource made available to the campus community for the purpose of conducting University business. These guidelines help establish uniform, campus-wide criteria for the use, content, and management of Public Folders so that their use will not present security vulnerabilities or impede the e-mail service's performance and stability. Inappropriate use of Public Folders, such as posting offensive, abusive, and/or harassing messages, will be reported to Human Resources Management for appropriate action, which may include disciplinary action and any legal action as required by California State Law. Using Public Folders indicates that you have read and will abide by these user guidelines.

2 Definitions

Confidential Information: In addition to those listed in the Personal Information definition below: financial records; medical records; physical description; home address; home phone number; education; grades; ethnicity; gender; employment history; performance evaluations; disciplinary action plans; NCAA standings; etc. Confidential information must be interpreted in combination with all information contained on the computer or in printed format to determine whether a violation has occurred.

NOTE


For more details about the confidential nature of student records, learn about the Family Education Rights and Privacy Act at: www.calstatela.edu/ferpa. To learn more about the legal aspects of confidential information, visit the ITS Guidelines and Policies web page: www.calstatela.edu/its/policies.

Personal Information: Under California Senate Bill (SB) 1386: The individual's first name or first initial and last name in combination with any one of the following: Social Security Number (SSN); driver's license number; California Identification Card; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Proprietary Information: Information that an individual or entity possesses, owns, or holds exclusive rights to. Examples include: faculty research; copyrighted materials; white papers; research papers; business continuity and other business operating plans; e-mail messages; vitae; letters; confidential business documents; participants of an organization, class, or group; detailed building drawings; network architecture diagrams; etc. Proprietary information, if lost or stolen, could compromise, disclose, or interrupt operations or embarrass the individual or the University.

Public Folder: A feature of Microsoft Outlook™; a type of electronic bulletin board that provides a way to collect, organize, and share information with others on and off campus.

Shadow Systems/Confidential Files: Any files or applications, third party or home-grown databases, systems, spreadsheets, documents, tables, etc., external to Student Administration (SA) and the Common Management System (CMS) applications and that contain personal and/or confidential information. Examples: Stand-alone payroll or financial systems; student housing systems; library

 User Guidelines for Outlook™ Public Folders	Guidelines No.	ITS-1002-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
	Page 2 of 6			

systems; rosters that contain names of students, their addresses, phone numbers, and grades; attendance databases containing emergency contact information; information repositories containing passwords, employee ID numbers, drivers' license numbers, and Social Security Numbers; and rosters containing NCAA standings or commuter information.

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
SB 1386	California Senate Bill 1386: Personal Information Privacy
ITS-1009-G	User Guidelines for Separated Employee's Network/E-mail Access
ITS-8808	Network / E-mail Account Request
ITS-8818	Department E-mail Account Request
ITS-8821	Outlook™ Public Folder Request

4 Guidelines


4.1 Public Folder Account Holder and Responsibilities

- a) Only those faculty, staff, and departments who have University e-mail accounts may apply for a Public Folder account using the *Outlook™ Public Folder Request*. The *Outlook™ Public Folder Request*, *Network / E-mail Account Request*, and *Department E-mail Account Request* forms are available online at: www.calstatela.edu/its/forms.

NOTE

The following individuals, groups, and organizations are **NOT** eligible to obtain a Public Folder:

- Students
 - Associated Students, Inc. (ASI)
 - Los Angeles County High School for the Arts (LACHSA)
 - Consultants or Vendors
- b) Public folders are granted to qualifying applicants. Once approved, the Public Folder account owner is responsible for the security, content, management, and housekeeping of the Public Folder. In addition, the account owner is responsible for ensuring that the Public Folder:
- Is used according to the guidelines set forth in section 4.2
 - Contents meet the criteria as set forth in section 4.4
 - Has security settings appropriate for the folder's contents, and that the folder is administered as outlined in section 4.5

 User Guidelines for Outlook™ Public Folders	Guidelines No.	ITS-1002-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
	Page 3 of 6			

- c) Public folders are renewable on an annual basis, and their account owners must reapply for them using the *Outlook™ Public Folder Request*. Public Folders that have not been renewed will be deleted.
- d) All network and e-mail access, including Public Folder access, ceases upon official separation from the University, and Information Technology Services (ITS) locks user accounts upon receipt of separation notification through the Human Resources Management (HRM) online separation form. Departments should be proactive and reassign designee rights prior to the separation date. The Public Folder account owner is responsible for immediately removing access when employees separate from the University. See Section 4.2 Changing Designees on Public Folders in *ITS-1009-G: User Guidelines for Separated Employee's Network/E-mail Access* (located online at www.calstatela.edu/its/policies).


4.2 Proper Usage

- a) Cal State L.A. Public Folders should be used only for legitimate University-related purposes.
- b) Assume that Public Folders are not secure. Never post personal, confidential, proprietary information, shadow systems, and/or confidential files to a Public Folder.

NOTE

Find information about the Family Education Rights and Privacy Act at www.calstatela.edu/ferpa, and about other laws and regulations regarding confidential information on the ITS Guidelines and Policies web page at www.calstatela.edu/its/policies.

- c) Do not post any item containing obscenities, harassment, threats, slander, or offensive comments regarding gender, race, religion, sexual orientation, or other protected categories, or any other inappropriate or unlawful content.
- d) Only post items that you have permission to post. Do not pose as someone else when posting any item.
- e) Invasion of privacy, unlawful access to confidential information, and posing as another person are actions that will be reported to Human Resources Management for appropriate action, which may include disciplinary action and any legal action as required by California State Law.
- f) Be cautious about what you post in a Public Folder. Although items can be posted and then deleted, consider that during the time they reside in the folder, items can be retrieved and/or forwarded to others.
- g) Respect copyrighted material. Do not reproduce and post any material unless all references, quotes, and sources are properly cited.
- h) Do not make changes to someone else's item and re-post it without clearly indicating where changes were made and by whom. Unidentified changes to another's items constitute misrepresentation and/or defamation.

 User Guidelines for Outlook™ Public Folders	Guidelines No.	ITS-1002-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
	Page 4 of 6			


- i) Since body language cues and verbal intonation are absent from written messages and documents, take care to achieve the proper tone when posting items to a Public Folder. Sarcasm and humor can be misinterpreted easily.
- j) The Public Folder functionality is a communications tool. It is not a replacement for a filing cabinet, media storage, or document retention system.

4.3 Privacy and Monitoring

- a) Items posted to a Public Folder are not private. Once an item is posted, the author and/or folder owner should have no expectations of privacy regarding it. The item can be forwarded to others, or printed and given to others.
- b) Mandatory disclosure of the contents in Public Folders is a possibility. For instance, posted items may be subject to production to people other than the intended readers pursuant to a Public Records Act request, a relevant civil litigation discovery request, or a subpoena.
- c) Public Folders are subject to internal monitoring if suspicion arises that its usage violates University policy.
- d) “Deleting items” actually may not be permanently deleted. Previously, items may have been retrieved and/or forwarded to others. And, it might be possible to retrieve deleted items from the University’s data backups.
- e) In some cases, access by certain individuals to a Public Folder may be restricted by the folder’s owner. To protect entry to your e-mail account, and thereby the Public Folders, secure your password. Do not share your password with anyone. If someone else gains access to your password, change it immediately.
- f) To prevent unauthorized users from accessing a Public Folder and forwarding items as if from you, always lock your computer (**Ctrl-Alt-Del + Lock Computer**) before you leave your workstation.

4.4 Folder Contents


- g) Public Folders are provided for the purpose of posting and reading documents such as:
 - Announcements
 - Bulletins
 - Calendars for reservations (such as conference rooms)
 - Departmental instructions and collaborations
 - Forms
 - Guidelines
 - Meeting notes
 - Procedures
 - Reports of general interest
 - Templates
 - Training schedules and materials

 User Guidelines for Outlook™ Public Folders	Guidelines No.	ITS-1002-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
	Page 5 of 6			

- h) Public Folders should only be used as a repository for materials of a “public” nature or general interest to all or a portion of the campus.
- i) Public Folders may not be used to store confidential and/or sensitive information, personal e-mail messages, or anything that violates federal or state laws and regulations or the University’s policies, procedures, and guidelines regarding the handling of confidential information and appropriate computer use.
- j) Public Folders should only contain current, up-to-date items. All expired or out-of-date material should be promptly removed.
- k) The maximum storage limit for a Public Folder, including all its subfolders, is 2 gigabytes (GB).
- l) Public folders should **never** be used as storage for any of the following:
 - E-mail messages, spreadsheets, lists, and/or documents that contain confidential and/or sensitive information
 - Personnel (employment) information
 - An individual’s e-mail messages
 - List serve or newspaper daily deliveries
 - Personal documents or messages
 - Test folders (i.e., folders used for testing something)
 - Information older than two years unless it is still pertinent (e.g., forms that have not been revised, instructions that are still in effect, etc.)
 - Information that is not of general interest to all or a portion of the campus

4.5 Folder Security and Administration

- a) The Public Folder account owner is responsible for allowing and restricting access to a Public Folder. After the folder is created, set up its security to match the folder’s contents. **Confidential information should never be stored in a Public Folder.** However, if the folder contains information for a limited audience, set the folder’s security to prohibit all those except your target audience from gaining access to it.
 - On the Outlook™ main menu, select **View ► Folder list**.
 - Right-click on your Public Folder and select **Properties**.
 - Click on the **Administration** tab:
 - *Drag and Drop posting* should be set at **Move/Copy**.
 - *This folder is available to:* should be set for **All users with access permissions or Owners only**, depending upon your security needs. Click on the **Apply** button after you have made your selection.
 - Click on the **Permissions** tab. Add users and assign/define their Permission Levels. Click on the **Help** button or press the **F1** key for assistance with this task. Click on the **Apply** button after you have made your selection. [Note: if you restrict this folder, the Default and Anonymous users’ Permission Levels should be set at

 User Guidelines for Outlook™ Public Folders	Guidelines No.	ITS-1002-G	Rev:	B
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Issued:	6/21/06	Effective:	6/21/06
				Page 6 of 6

None. If your folder is not restricted, keep the Anonymous user's Permission Levels at **None**, and the Default users as **Reviewer**.]

- b) If folder access is restricted, the Public Folder account owner is responsible for ensuring that those on the Permissions list know the folder "rules." For example, if items should not be forwarded, this should be communicated to those using this folder. All individuals with access to a Public Folder should be expected to abide by the folder restriction(s) or lose their access privileges. All users are expected to adhere to all the user guidelines contained in the herein document.

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

- a) Questions regarding these guidelines should be directed to itsecurity@calstatela.edu.
- b) Technical problems related to a Public Folder or the Outlook™ Public Folder Request should be directed to the ITS Help Desk (LIB PW Lobby), extension (323) 343-6170.