

TRANSFER GUIDELINES

for

E-Mail Records



Prepared by the Collaborative Electronic Records Project
Rockefeller Archive Center
Revised December 2008

This document may be freely used and modified by any non-profit organization.

TABLE OF CONTENTS

Introduction	3
<u>Section I – Guidelines for Depositing Organizations</u>	
Selecting Records for Transfer to the Archives	6
Transfer Instructions	8
Depositor Information Form	10
<u>Section II – Guidelines for Accessioning Archivists</u>	
Pre-Accessioning & Appraisal	13
Accessioning	15
Transfer	15
Processing	18
Changes	18
Storage	18
Disposal	18
Appendix 1 – Preservation Formats for Electronic Records	19
Appendix 2 – Desktop Search	22
Appendix 3 – E-Mail Search	26
Appendix 4 – Depositor Transfer Preparedness Survey	32
Appendix 5 – DoD Compliant Records Management Software	36
Appendix 6 – Setting up .pst files	38
Appendix 7 – Electronic Records Accession & Documentation Form	44
Appendix 8 – Electronic Records Transfer Form	47
Appendix 9 – Electronic Records Verification Form	48
Appendix 10 – Electronic Records Refresh/Migration Schedule	49
Appendix 11 – Glossary	50

INTRODUCTION

In August 2005, the Rockefeller Archive Center (RAC) launched a three-year Collaborative Electronic Records Project in partnership with the Smithsonian Institution Archives. The project's primary objective is to develop management guidance and technical preservation methods that will enable archives to make electronic information accessible and usable for future researchers. To accomplish this goal, depositing organizations will need to establish policies and procedures for generating and saving electronic information long before records are transferred to an archive. By raising awareness among donor organizations when electronic records are being generated rather than waiting until the records are deposited, the RAC hopes to receive electronic records with their authenticity and integrity intact.¹

This document sets forth archival methods of preparing electronic records for transfer to an archive, and may be adopted, in whole or in part, by any non-profit organization; however, it is written as though the depositor were transferring records to the RAC. Circumstances may dictate modification to fit the needs of a particular office. Before implementing these guidelines, each organization should review them and their Records Management Policy with legal, financial, information technology, and administrative advisors.

Both the information technology and archival professions recommend using specific, technology-neutral file formats for long-term archival storage of electronic records because those formats have been in use so long and by so many companies that they have become standard and because they are expected to continue to be in widespread use. Ideally a record should be created in the preferred format or migrated to that format as soon as possible after creation.

The most common electronic record formats are listed in Appendix 1 with corresponding preferred long-term preservation formats. Secondary preservation formats are indicated in the event the primary preservation format cannot be used. Depositors should convert their electronic records to one of the preferred formats

¹ Authenticity means a record that is what it purports to be, i.e., includes the e-mail with its attachments and transmission data, and that was created by the credited author. Integrity is confirmation that a record has not been altered, intentionally or accidentally, since its creation or receipt.

prior to depositing them with the Rockefeller Archive Center. If unconverted electronic records are deposited with the Archive, its staff will attempt to preserve the records received by conducting the format conversion on a copy of the received records. Successful transformations will be verified and subsequently archived in addition to the original record. Please note that conversion efforts may be unsuccessful, especially if attempted years after the records were created. **Personal or confidential material should be removed before the records are deposited as the Archive Center cannot guarantee that such items will be identified or removed after transfer.**

Non-permanent records should not be transferred to the Archive. Rather, they should be retained by the Depositor or placed in on-site or offsite short-term storage for the duration of their proscribed retention period. When the destruction date arrives, temporary electronic records should be shredded or have the data completely destroyed via other acceptable means such as a software program that removes all traces of files.²

Electronic information that is considered a permanent record may include text, images, video, brochures, manuals, meeting proceedings, websites, journals, calendars, e-mail, distribution lists, and voice mail. Data may be on desktop hard drives, servers, employee's home computers, floppy disks, diskettes, CDs, DVDs, thumb drives, Blackberries, or other removable or remote devices. Regardless of their location, permanent records should be backed up on the server and should be organized in a consistent, logical manner throughout the company, and should mirror that of corresponding paper records.

² One such program is Eraser by Tolvanen at <http://www.tolvanen.com/eraser/>. For more complete information, see "Records Retention & Disposition Guidelines" published by the RAC and CERP at <http://siarchives.si.edu/cerp>.

SECTION I

GUIDELINES FOR DEPOSITING ORGANIZATIONS

SELECTING RECORDS FOR TRANSFER TO THE ARCHIVE

Your organization's Records Management Policy and the Records Retention and Disposition Guidelines should guide selection of electronic records to be retained permanently and transferred to the RAC.³ Your organization's management team should work with the RAC e-mail accessioning archivist to determine which e-mail folders from which staff members will be routinely captured at what intervals for transfer to the Archive.

E-mail records transferred to the Archives should:

- ▶ Be of official or historical value;
- ▶ Be "Office of record" materials, meaning that the office is the creator of the file or is the primary recipient of the e-mail that originates from external organizations;
- ▶ Be only those records original to your department or that you play an active role in creating;
- ▶ Be neither recently created nor regularly accessed (rule of thumb: over 90 days old or accessed less than five times annually);
- ▶ Include transmittal e-mail when an e-mail transmits an attachment that is a record. This is required for legal purposes to verify authenticity and integrity.

Do **NOT** transfer:

- ▶ E-mails containing information that is also found in a report or other document that will be transferred to the Archive;
- ▶ Messages with prior threads of a discussion (as well as pertinent attachments) when a final e-mail includes prior threads and attachments;
- ▶ Drafts (unless they contain significant comments or annotations that indicate reasons for decisions or actions);
- ▶ Routine Correspondence, e.g. meeting announcements, address changes, invitations, acknowledgments, reservations, confirmations, travel itineraries, holidays, vacation schedules, and routine requests for general information;
- ▶ Routine Administrative Records, e.g. purchase orders, travel vouchers,

³ If your organization does not have its own, you may use "E-mail Guidelines for Managers & Employees" and "Records Retention & Disposition Guidelines" developed by the Collaborative Electronic Records Project: <http://siarchives.si.edu/ceerp>.

requests for building services and maintenance, time sheets, applications for leave, training files, etc.;

- ▶ E-mail advertisements and promotional materials from vendors and similar messages generally considered SPAM (unsolicited, commercial e-mail, sent to a mass mailing list);
- ▶ Messages to/from ListServes not pertinent to your organization's operation, policies, or programs;
- ▶ Messages and attachments containing viruses; viruses should be cleaned or the messages quarantined for review by an archivist;
- ▶ Personal and confidential e-mail messages and content subject to privacy laws.

NOTE: any personal, confidential, sensitive messages transferred to the RAC will be subject to viewing and use by Archive Center staff and possibly future researchers, although Archive Center staff will make reasonable attempts to identify and remove such messages.

Soon after creating or receiving an e-mail, your designated keeper(s) of the official copy of e-mail records should have placed the official copies in the proper, pre-determined organization folders that are established as part of your regular workflow process. For example, folders may include "Staff Meeting Minutes_2008", "Program Development_Arts", "Press Releases_2006." Some records may require sub-folders, e.g.:

Grants_Africa
Education.2008
Food.2006
Food.2007
Health.2004

To search for permanent record messages pertaining to a particular topic that may not be filed within proper folders, obtain your IT staff's assistance for efficiently locating those either by person, department, or organization-wide. In addition to or alternatively, use the Desktop and E-Mail Inbox searches shown in Appendices 2 and 3, respectively.

At the agreed upon capture dates (e.g., semi-annual on June 15), the official record keeper(s) and your Information Technology staff should identify folders ready for transfer to the RAC and should advise the RAC archivist.

TRANSFER INSTRUCTIONS

Your organization's Records Manager (or other assigned staff member) should be responsible for transferring files to the RAC. Please contact an archivist for assistance if needed, particularly if you have no Information Technology staff.

Steps

1. **Review Records Retention Schedule** to determine which records should be disposed of and which permanent records may be transferred to the RAC. If you have no records retention guidelines, you may use the CERP guidance publication available at <http://siarchives.si.edu/cerp>.
2. **Identify the record groups to be transferred**, including e-mail account owners' names, folder names, byte size, and date range. The Depositor Information Form following may be used.
3. **Advise the employees** whose records will be transferred to delete personal and SPAM messages and to sort confidential and sensitive messages to a separate folder, so identified. Employees should also confirm that all permanent records are appropriately organized and accessible and that records on portable devices such as thumb drives and Blackberries have been integrated.
4. **Prepare a document describing how each creator's records are organized**; the Depositor Information Form below may be used. A screen shot of their Inbox and Sent folders and subfolder structure will be helpful.
5. **Contact the accessioning archivist** to advise that you would like to prepare for the transfer process and to obtain any special instructions or assistance, particularly regarding e-mail format.
6. **Run virus scans** on original material, and, if any are found, use appropriate methods of removing viruses or quarantining infected messages before copying or transferring. If your staff does not have the expertise to do this, please discuss with the accessioning archivist.
7. **Determine if personal, confidential, sensitive, and SPAM messages have been removed**, and, if not, remove such messages to separate folders so marked. If the confidential and sensitive messages will ever be open for research, they may be transferred to the RAC in folders identified as "Sensitive" with an "open on" date specified; if they will be permanently closed, they may be transferred in folders so marked. (This step is best done after virus scanning as virus checks may identify more personal and SPAM messages.)

8. **Integrate records on portable devices** if employees have not done so.
9. **Determine if any files are encrypted or password protected**, and, if so, unencrypt or obtain encryption code(s) and password(s).
10. **Identify any copyrighted material** and document details regarding owner, contact information, and date of copyright.
11. **Make a digital copy of the files** as a precautionary measure and retain until the archivist confirms transfer is complete and verified.
12. **Identify the e-mail application and attachment file formats included.** If any are not in the preservation formats specified in Appendix 1, copy the files and attempt conversion on the copy. Document actions taken and advise the accessioning archivist.
13. **Refresh outdated removable media.** If records to be transferred are on removable media, *copy* records from 5.25” floppy disks, 3.5” diskettes, or other outdated removable media onto a server for capture, or to CDs or DVDs before sending to the RAC. Labeling – Do not write directly on CD/DVDs unless using an archival soft tip pen and then write only on the clear center hub of the top side. Do not apply labels to optical media.
14. **Document any actions taken** after record creation, listing who authorized the actions as well as what was done.
15. **Complete and sign the Deed of Gift or Deposit Agreement.**

Access by Researchers

The RAC will provide access to researchers in a read-only form, subject to conditions and restrictions outlined in the Deed of Gift or Deposit Agreement.

Contact Information

For questions or assistance with transferring electronic records to the RAC, call 914-631-4505 or e-mail archive@rockarch.org.

DEPOSITOR INFORMATION FORM for E-MAIL ACCESSIONS

E-mail Account Owner (Record Creator): _____

Job Title & Department: _____

Depositing Organization: _____

Record Group(s)/Series: _____

(Please attach a description of records organization, e.g. screen shot of Inbox or desktop folder tree.)

Date range _____ E-mail duplicated in paper records: Yes _____ No _____

Name of Records Management Software (if applicable) and version(s):

Operating system and version(s) (e.g., Microsoft Windows NT v4.0):

E-mail application(s) and version(s), (e.g. Microsoft Outlook 2003):

Attachment formats and versions:

Source of records: Desktop hard drive _____ Server _____ Removable media _____

Transfer method & format (CD, file transfer protocol (ftp), .pst, mbox, etc.)

Any files compressed? Yes _____ No _____ Encrypted? Yes _____ No _____
(If so, separately list files and provide details including method and application used to compress and supply encryption key.)

Copyrighted? Yes _____ No _____ If so, provide details separately.

List of senders and recipients attached (including those on distribution lists):

Yes _____ No _____

(NOTE: Show real names if not shown in e-mail address, e.g. rharm@npft.org - Robert Harmon.)

Folder/subfolder titles	Byte size	# Files/Attachments
-------------------------	-----------	---------------------

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Form completed by: _____

Title: _____ Date: _____

SECTION II

GUIDELINES FOR ACCESSIONING ARCHIVISTS

WORKFLOW

Due to the ephemeral nature of born-digital information, and because some depositing organizations do not have Records Management or Information Technology staff, designated archivists will need to work closely with depositors to appraise, capture, transfer, and accession electronic records soon after permanent records are created. In order to retain the authenticity, integrity, and longevity of digital records, best practices procedures should be followed carefully. The number of data conversions should be kept to the minimum required for preservation as there is always a possibility of data loss. Please read this entire section before transferring records.

Pre-Accessioning & Appraisal:

1. **Determine depositor's transfer readiness.** Before the first electronic records transfer from the depositor, have the depositor complete a Transfer Preparedness Survey (see Appendix 4), and discuss with the depositor any issues that arise from the answers provided.⁴
2. **Identify records to be transferred.** Review at least a sampling to determine the content is desirable material.
3. **Integrate records on portable devices.** Text messages and data on devices such as Blackberries and "thumb" drives should be consolidated into proper folders with other e-mail records.
4. **Determine retention period for records being transferred.** If the depositor has no Records Retention and Disposition Guidelines, the archivist should review the CERP guidance publication with the depositor to establish a retention schedule for the organization.⁵
5. **Determine if personal, confidential, sensitive, and SPAM messages have been removed.** If the depositor has not removed these messages, review Section I of this document with them. Personal and SPAM messages should be deleted. If the confidential and sensitive messages will ever be open for research, they may be transferred to the RAC in folders with "Sensitive" and an "open on" date specified in the folder names; if they will be permanently closed, they may be transferred in separate folders so marked.

⁴ See also "Depositor Survey—Electronic Records Status"
http://siarchives.si.edu/cerp/Depositor_E-Recs_Survey.pdf.

⁵ See "Records Retention & Disposition Guidelines" published by the RAC and CERP at
<http://siarchives.si.edu/cerp>.

6. **Obtain a list of folder names** including byte size, number of files, and date range of records being transferred (see Depositor Information Form in Section I).
7. **Determine and document how the depositor's records are organized.** If the depositor has not organized records they want to transfer, review Section I of this document with them.
8. **Identify the file formats included.** If any are not in the preservation formats specified in Appendix 1, work with the depositor to accomplish conversion on a *copy* of the records and document actions taken on the Accession and Migration Forms (Appendices 7 and 10). The secondary formats should be used only when the preferred formats are not possible.
9. **Identify any encrypted and password protected files.** If any files are encrypted, they must be unencrypted, and password protections removed before accepting records for transfer. If this cannot be done, the files should not be accepted. Alternatively, the RAC may decide to accept the files on the condition that they may be destroyed at the discretion of the RAC if later attempts to access the information are unsuccessful.
10. **Identify any copyrighted material.** Obtain details including owner's name, contact information, and copyright date. Record data on the Accession Form and later in the administrative and descriptive metadata.
11. **Have depositor copy records** (in digital, native formats exactly like originals). Files should be *copied* to desktop, server, or removable media before actual transfer as a precautionary measure in the event problems occur during transfer.
12. **Refresh outdated removable media.** Have depositor *copy* records from 5.25" floppy disks, 3.5" diskettes, or other outdated removable media to a server for capture, or to new CDs or DVDs before sending to the RAC. Labeling – Do not write directly on CD/DVDs unless using an archival soft tip pen and then write only on the clear center hub of the top side. Do not apply labels to optical media. Alternatively, identifying information may be written on the Tyvek envelope fold-over tab, using an archival soft tip pen.⁶
13. **Document changes.** Document any actions taken during appraisal, listing who authorized the actions and what was done (see Appendices 8, 9, & 10).

⁶ Refer to "Care and Handling of CDs and DVDs" by Fred Byers at <http://www.itl.nist.gov/div895/carefordisc/CDandDVDCareandHandlingGuide.pdf>.

Accessioning:

1. **Complete an Accession & Documentation Form** (see Appendix 7). Although the archivist will assign RAC unique accession numbers for each acquisition, the Archive's automated processor will assign a different unique identification number to each digital record.
2. **Complete a Deed of Gift or Deposit Agreement.**

Transfer:

Discuss with the donor the logistics for transfer (e.g., whether an RAC electronic records archivist or IT staff member will go to the donor's location or the donor's records manager or IT personnel will copy and deliver to the RAC.)

If the depositor uses a Microsoft Exchange server, the regular e-mail mailboxes "live" on the server, and thus can be captured from there. For organizations with other servers, if employees have set up Personal (folders individually created and named by the employee) or Archive folders (automatically mirroring folders in the Inbox) within their mailboxes, those folders are not part of the server backed-up mailbox. Personal and Archive files, if selected for transfer to the RAC, will have to be captured from desktops or first copied to the depositor's server.

- Removable media should be hand delivered by trusted courier, RAC electronic records archivist, or donor's records manager.
- E-mail messages on a personal desktop or laptop computer, network drive, or shared server may be transferred to the RAC on removable media (e.g. CD/DVD, external hard drive, thumb drive).

Copying to Removable Media:

- Use archival quality gold CD+/-R or DVD+/-R discs or an external hard drive.
- If transferring Microsoft Outlook e-mail, extract messages and attachments into PST files to conserve space on removable media for transfer to the RAC.⁷ Preferably, the Information Technology staff for the depositing organization will convert to PST format at the server level; however, individual employees whose e-mail is being transferred may make the conversion to PST on their desktop hard drives. See Appendix 6 for instructions.
- If transferring e-mail other than Outlook, you may copy in the native, source format without extracting messages or attachments.

⁷ PST is Personal Storage File, a Microsoft Outlook proprietary format that creates one file containing all selected e-mail messages and attachments. It is stored outside of the e-mail server.

- Encrypt data if using an external hard drive or thumb drive and unencrypt upon arrival and accession at the RAC.
- Sanitize (using DoD approved software and methods) external hard drives and thumb drives before reusing.

(Do not use DAT or other magnetic tape as data can be overwritten or corrupted.)

- Immediately upon receipt, the RAC electronic archivist should make 2 copies – one read-only for permanent retention and one rewritable for editing by the archivist to remove personal, confidential, non-business messages.

E-mail files received on removable media:

Records RAC previously received on 5.25” floppy disks, 3.5” diskettes, or other outdated removable media should be copied (refreshed) to new, preservation quality media such as gold CDs or DVDs or directly to the RAC’s secure server dedicated to electronic records storage. Format migration may also be needed. See E-Mail Processing Guidelines.

1. **Check to be sure the e-mail transferred in its native format.**
2. **Check to be sure that automatically generated metadata transferred** with each message. For example, on a Microsoft Outlook toolbar, with the original e-mail open, select View, then Options, and see the “Internet Header” information in the dialog box. On the copied e-mail, select File, then Properties, then the Details tab.
3. **Check to be sure each part of the e-mail message is identified**, including: Date, To, From, Subject, Message, Attachment, as well as transmission and receipt metadata (time sent, time opened, message size, file name, etc.).
4. **Check to be sure e-mail has delimiters** indicating the beginning and end of each message and attachment.
5. **Check to be sure each attachment is differentiated** from the e-mail message and has its own unique identifier.
6. **Check to be sure all recipients are identified** even those “blind” copied. If the person’s actual name is not part of the “To” information automatically shown, the e-mail transfer should include a list identifying senders and recipients for each e-mail address. Distribution lists should also be included with each member’s name and individual e-mail address specified.
7. **Make backup copy(s).** Immediately after transfer, make at least one copy of the records to use as the “working” copy, leaving the original as the “official” record. Ideally, one backup copy should be on preservation quality gold CD/DVD and stored off site; a second copy should be retained on site, either on a separate server or on removable media.

8. **Perform a virus check** on the working copy on an isolated computer (one that is not used for other daily work and not one that contains stored records). Note that some anti-virus programs will not effectively scan mbox format. It is recommended that at least two anti-virus programs be used and that both the native format and .eml versions be scanned.
 9. **If viruses are discovered**, attempt to remove or quarantine the infected messages/attachments. Verify that the removal/quarantine did not alter remaining data by opening in Notepad or a web browser and sampling messages in the original and the copy.
 10. **Document virus actions** on the Verification Form (Appendix 9).
 11. **Document transfer** on Transfer Form (Appendix 8).
 12. **Verify** that the copy contains the same byte size and number of folders and files by right clicking on the folder, then selecting “properties.” Open the original transfer and a copy in Notepad or a web browser and sample the copy at various points to be sure the copied data is readable and matches the original.
 13. **Document your actions** on the Verification Form (Appendix 9).
 14. **Advise depositor** that their contingency copy may be destroyed in accordance with guidelines in their Records Disposition Manual.
- In the future, RAC may have File Transfer Protocol (ftp) or secure server transfer options, thus those methods are included below.

Secure Server Transfer (preferred method, if possible):

Obtain assistance from RAC and depositor’s IT staff.

File Transfer Protocol (ftp):

Obtain the following information from the depositor:

- ▶ IP address for the Depositor’s FTP site
- ▶ A temporary user name and temporary password with read-only privileges for use in accessing the Depositor’s FTP site
- ▶ Stipulate Windows, Unix, or Linux format
- ▶ A designated time or time span for the RAC to access the records and download a copy
- ▶ Check with IT staff regarding limitations on the size of FTP transfers
- ▶ If files are not copied from the server, be sure to retrieve any attachments that do not reside on the source drive or media.

Zip format is acceptable ONLY if zero compression is used, full file name is used (do not truncate to 8.3 naming convention), and full file path is kept.

Do not compress files (including databases) unless the compression method is “lossless,” such as LZW. (One lossless compression application is StuffIt Deluxe; version 9 is recommended although version 7.5 is acceptable. The filename extension will be *.sit.) If compression is used, a description of the method and application used must be included in the transfer documentation. Also all hierarchical file mappings and relationships must be included with the compressed file. For example:

Archive of Technical Notes

C:\Technical Notes\index.pdf

C:\Technical Notes\IT-971\

C:\Technical Notes\IT-971\IT-971-01.pdf

C:\Technical Notes\IT-920\.

Processing:

See Workflow and E-Mail Processing Guide and CERP E-mail Parser User Guide.

Changes:

Document any actions taken and decisions made during and after initial processing, listing who authorized the actions and decisions as well as what was done (see Appendices 8, 9, & 10).

Storage:

If records will not be processed immediately, both the original digital records, the copies, and related accessioning and transfer forms should be archived together in an electronic folder, with each component clearly identified and properly stored according to the RAC’s processing guidelines for electronic records. Originals may be kept: 1) on a dedicated server (recommended) in a secure space; 2) on removable media; or 3) placed in a digital repository such as DSpace or Fedora, all with access limited to authorized archivists. One copy should be stored offsite.

Disposal:

It is not anticipated that the Archive Center will dispose of digital records during the transfer process; however, in the event a situation arises that requires disposal (such as SPAM or personal content), an appropriate method should be used and the event documented. See “Records Retention & Disposition Guidelines”

<http://siarchives.si.edu/cerp>.

APPENDIX 1

Preservation Formats for Electronic Records*

Original/Creating Application	Primary Preservation Format	Secondary Preservation Format
Various (.txt)	ASCII (keep original extension)	PDF/A-1-a
Corel WordPerfect (.wpd, .wpx, .doc, .rtf)	PDF 4.0 or higher PDF/A-1-a	Rich Text Format (.rtf)
Microsoft Word (.doc, .dot, .rtf)	PDF 4.0 or higher PDF/A-1-a	Rich Text Format (.rtf)
Lotus 1-2-3	Same as original	Comma Separated Variable (CSV)
Microsoft Excel (.xls)	PDF/A-1-a	CSV PDF
Microsoft PowerPoint (.ppt)	PDF/A-1-a	PDF
E-mail	Generic (.mbox) or (.eml)	Outlook Archive (.pst, .html); Plain Text (.txt)
Graphics Applications		
Various graphics applications (.bmp, .tif, .jpg, .gif) Macromedia Fireworks Freehand (.png)	TIFF (24-bit RGB) (minimum 3000 pixels along long dimension or 400 dpi, whichever is greater) PNG/JPEG (raw)	JPEG (uncompressed) (for JPG and GIF formats only.) TIFF (8-bit, grayscale or b/w for black and white images only) (minimum 3000 pixels along long dimension or 400 dpi, whichever is greater)
Adobe Photoshop, Illustrator (.psd, .eps)	TIFF (24-bit RGB) (minimum 3000 pixels along long dimension or 400 dpi, whichever is greater)	

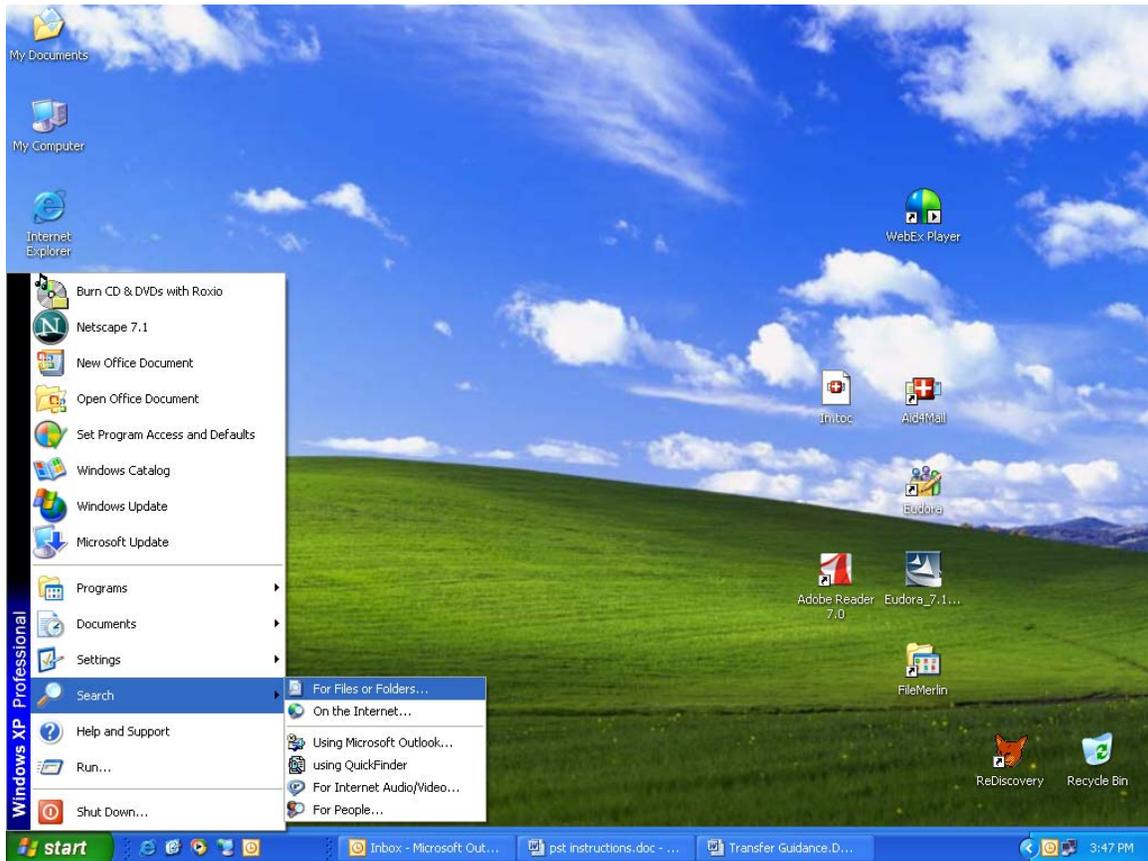
Graphics Applications (cont.)		
Microsoft Publisher (.pub) Microsoft Image Composer (.mic)	TIFF (24-bit RGB) (minimum 3000 pixels along long dimension or 400 dpi, whichever is greater)	TIFF (8-bit, gray-scale or b/w for black and white images only) (minimum 3000 pixels along long dimension or 400 dpi, whichever is greater); convert TIFF to PDF/A-1-a if necessary to reduce file size
Database Management Systems (DBMS)		
Dbase III+ (.dbf, .dbt)	Same as original	CSV
Lotus Notes (database)	Same as original	CSV
Microsoft Access (database) (.mdb)	Same as original	CSV
Microsoft SQL Server (.bak)	Same as original, full backup made with MS SQL	CSV
Sybase SQL Server, Adaptive Enterprise Server, SQL Anywhere	Same as original, full backup made with Sybase dbms. Also requires full backup of Sybase master database.	CSV

WebPage Developers and HTML Editors		
Adobe PageMill, Microsoft Frontpage, Macromedia Dreamweaver; other (.htm, .html, .shtml)	XHTML 1.0	PDF (Isolated, single webpage only)
Active Server Page (various) (.asp)	XHTML 1.0	ASP (depending on parameter complexity)
Macromedia Cold Fusion (.cfm)	XHTML 1.0	
Macromedia Flash/Shockwave (.swf)	Same as original	Analyze carefully for embedded URLs or other file dependencies.
Real Media (.rm, .ram)	Same as original	
Architectural Design/Engineering Graphics		
AutoCAD (.cad)	PDF (v6.0 with layer retention)	CGM; Web CGM; DWF
Microsoft Visio (.vsd)	PDF/E SVG 1.1 (.svg)	
Audio	AIFF (uncompressed) (.aif, .aiff) WAVE (LCPM only) (.wav)	AIFC (.aifc) WAVE (compressed) (.wav)
Video	MPEG-1; MPEG-2 (.mpg, .mpeg)	Ogg Theora (.ogg) AVI (.avi) Quick Time Movie (.mov)

*Table based primarily on one used by Smithsonian Institution Archives. Choice of the preferred formats was based on their maturity, widespread use, longevity, adherence to industry standards, and capability of displaying content that appears as much like its original format as is feasible.

APPENDIX 2

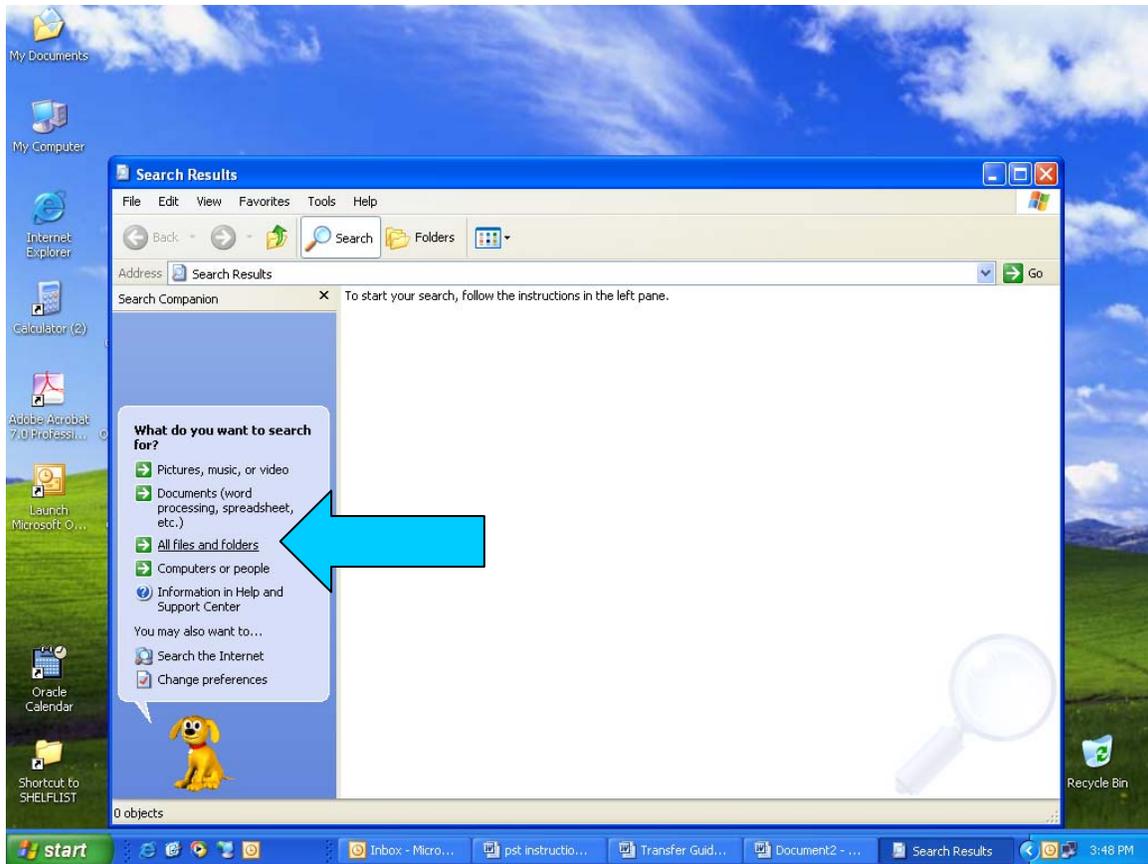
Desktop Search



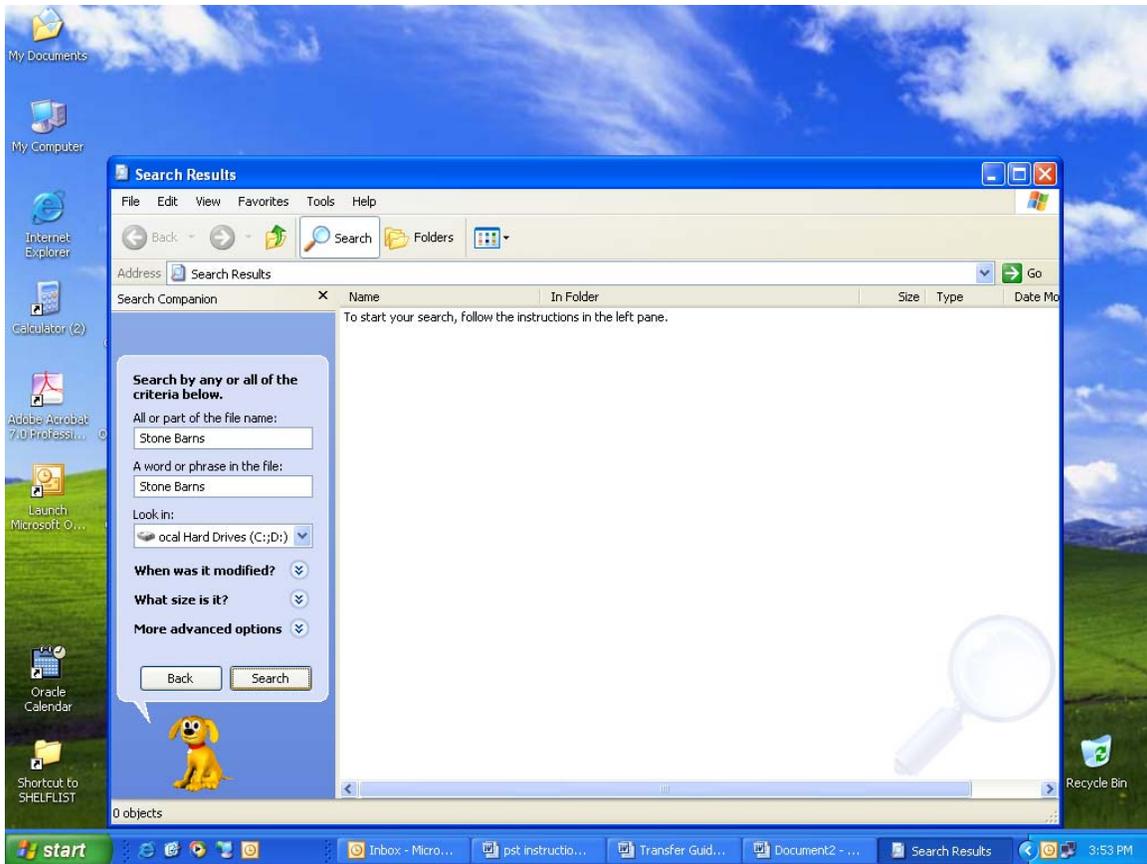
Click on the Start button in the lower left hand corner

Select “Search”

Select “For Files or Folders”

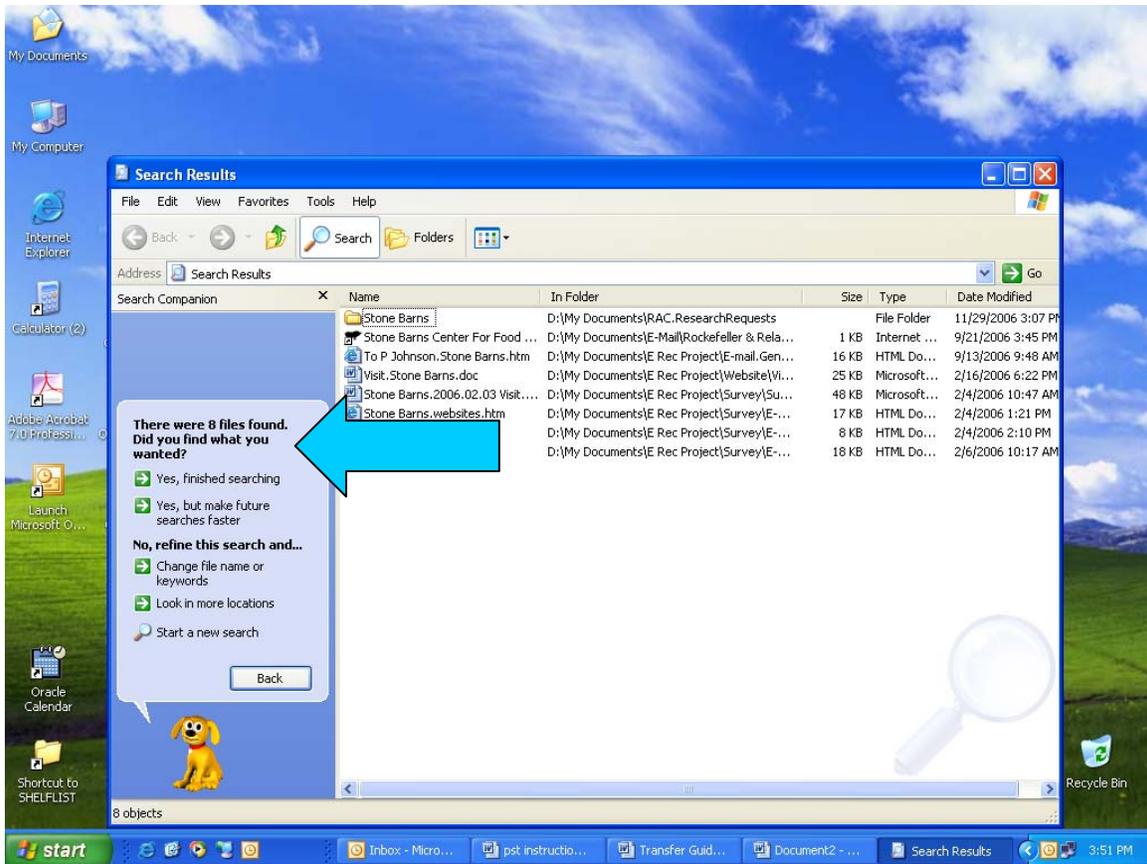


Select “All files and folders” (or another of the choices if appropriate).



Enter the file name and/or word you want to search for and choose the drive you want to search. You may also narrow the search by choosing one of the three questions in bold and selecting from among the drop down menu choices.

Click on “Search.”



The search dialog box indicates 8 files were found and the screen shows each with its related file path and other pertinent information.

From here, you could select the file(s) you want to transfer to the Archive and either:

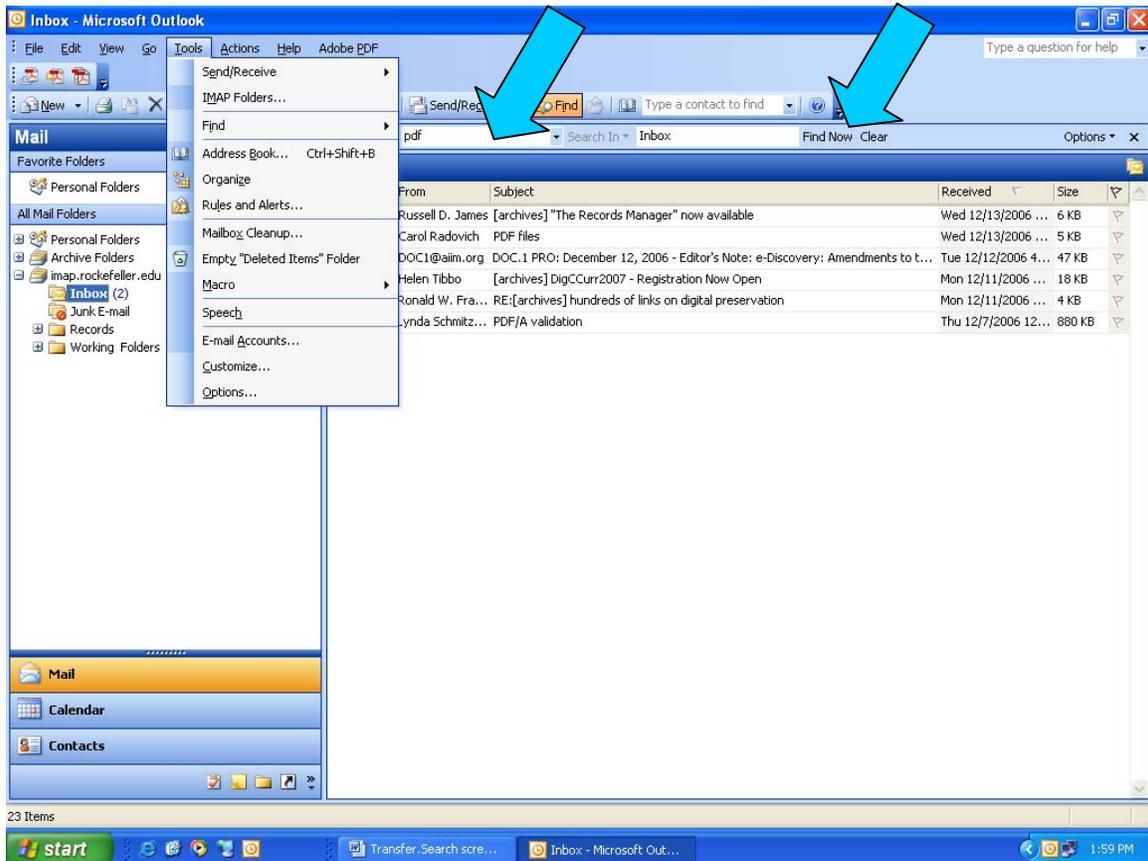
- 1) Open / File / Save As and enter the drive, folder, file name to save under

Or

- 2) Go to Windows Explorer, open the folder and/or file and right click and drag (copy) to the folder and drive where you want to save it

APPENDIX 3

E-Mail Search



E-mail Inbox and Sent Mail (MS Outlook):

Under "All Mail Folders," highlight the folder you want to search in

On the toolbar, select "Tools"

"Find"

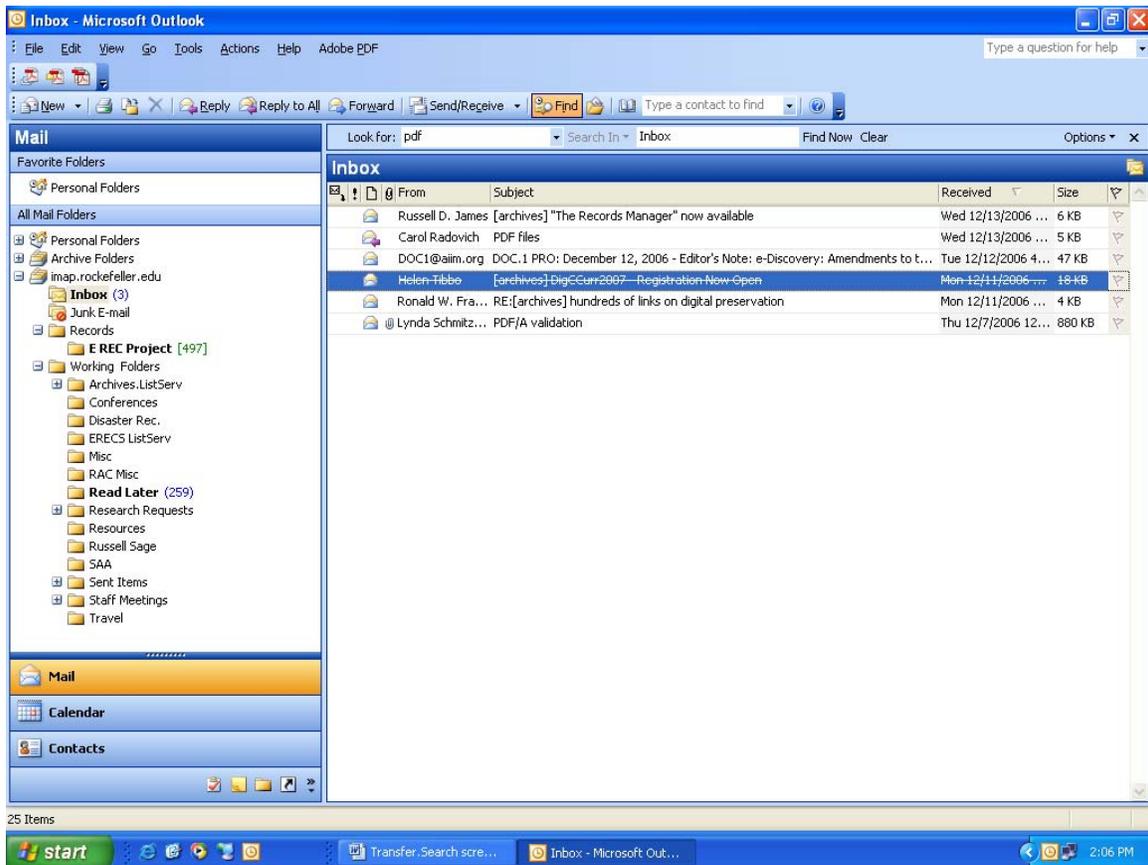
and "Find" on the next screen

In the "look for" box, enter search term e.g. "pdf"

Click on "Find Now" box

"Clear" will appear beside the "Find Now" box indicating that the search is complete.

Results of search are shown in above screen - 6 messages with the search term in the subject line or message text



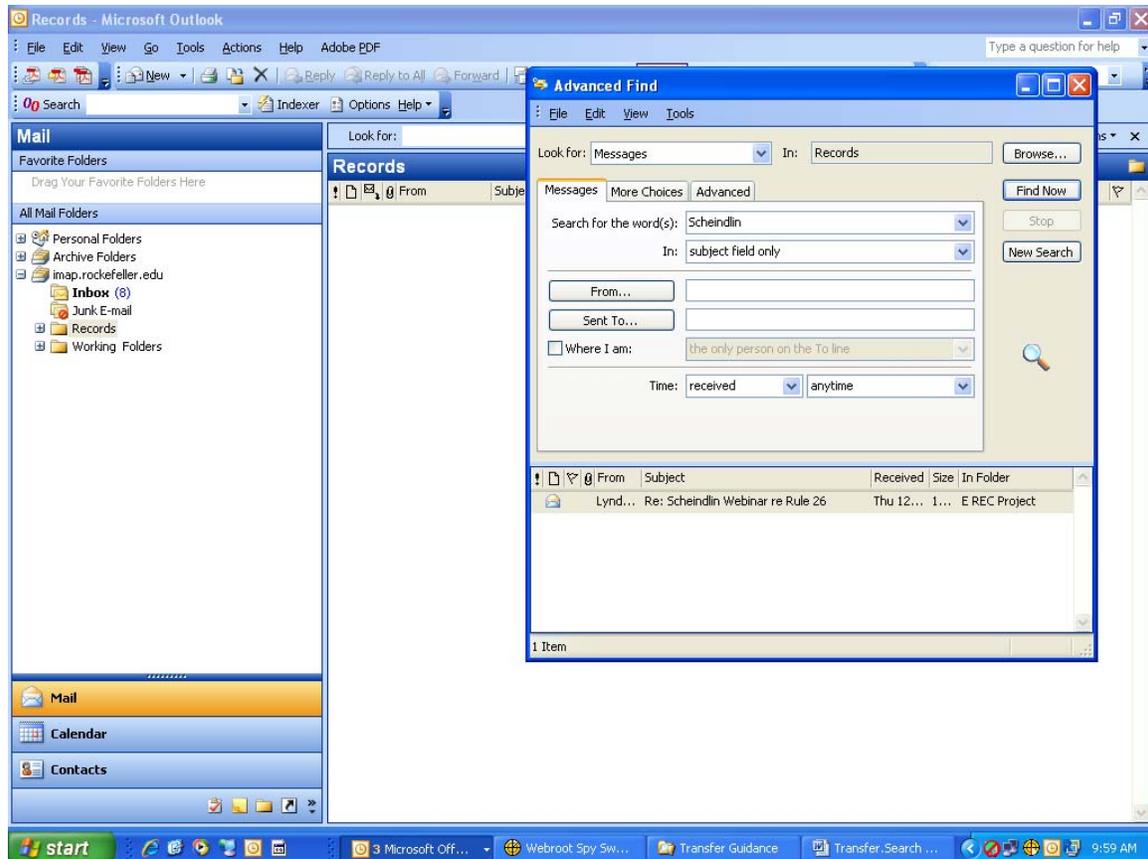
Click and drag messages to the appropriate folder for capture and transfer to the Archive. If you want to copy in lieu of moving the messages, press CTRL on the keyboard while dragging the items. The cursor will show an attached envelope outline with a + sign indicating that the items are being copied.

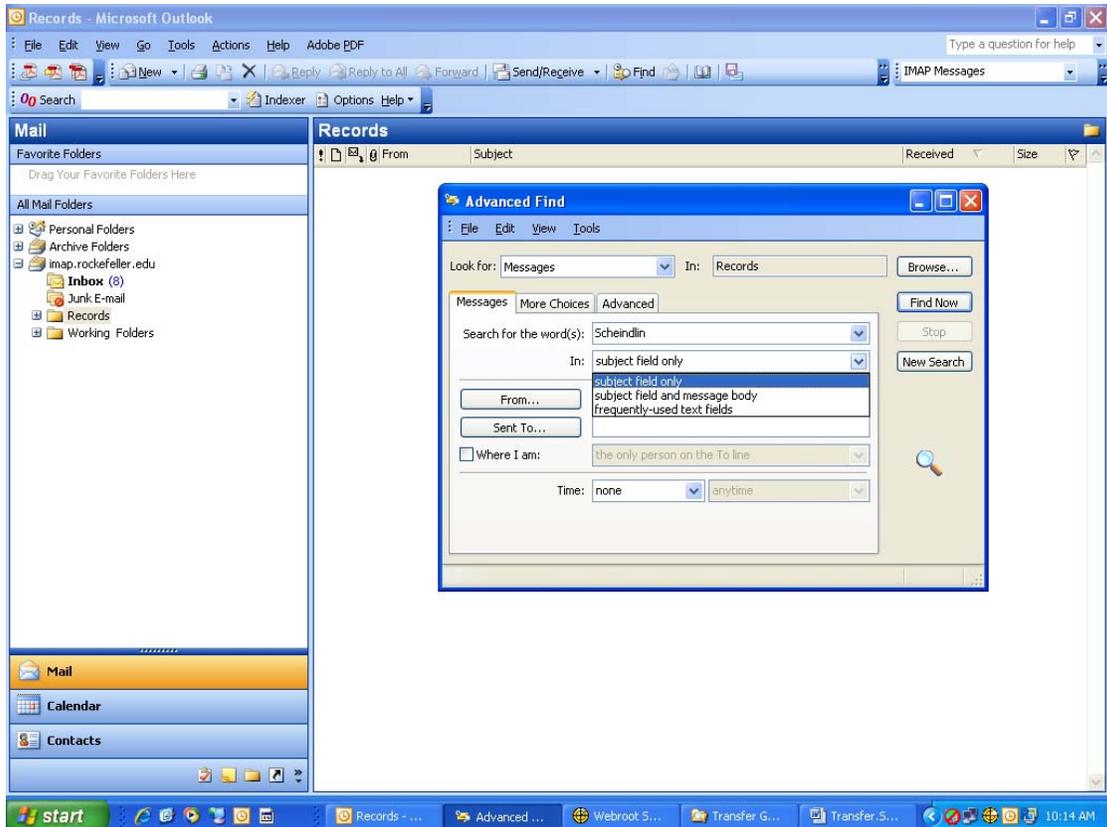
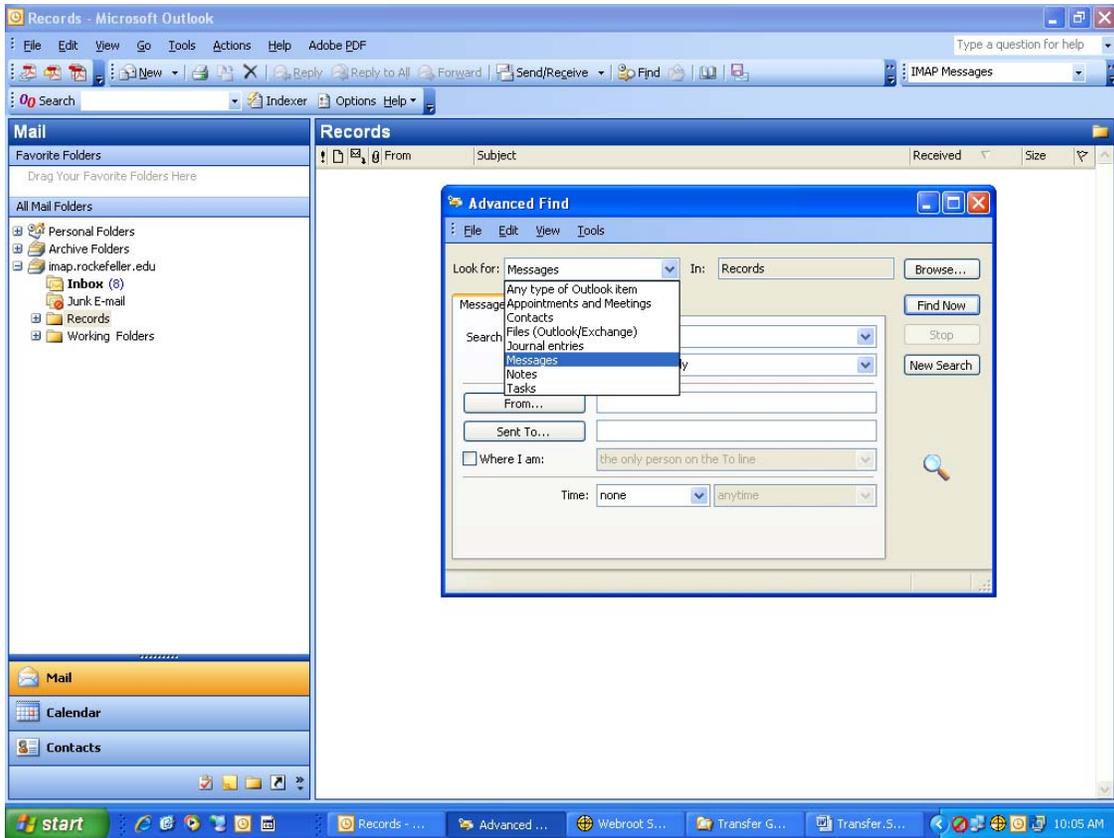
If you want to move or copy all folders found, on the toolbar select Edit, then Select All.

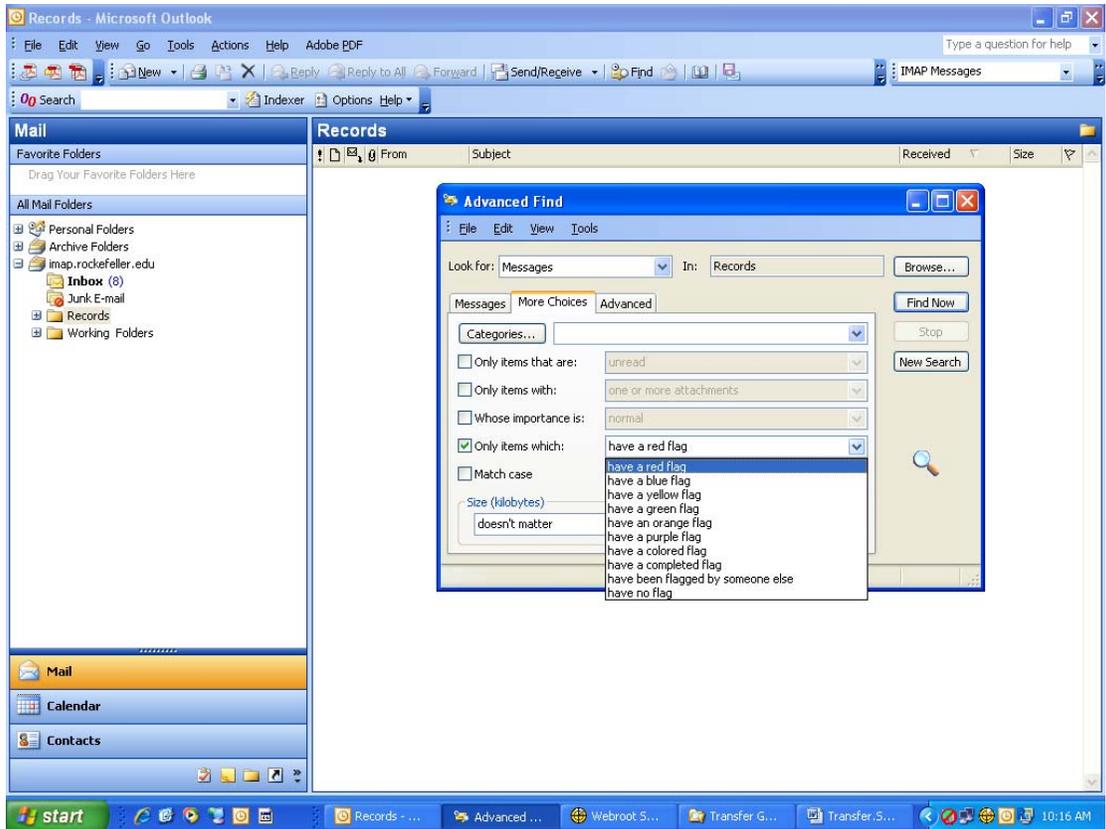
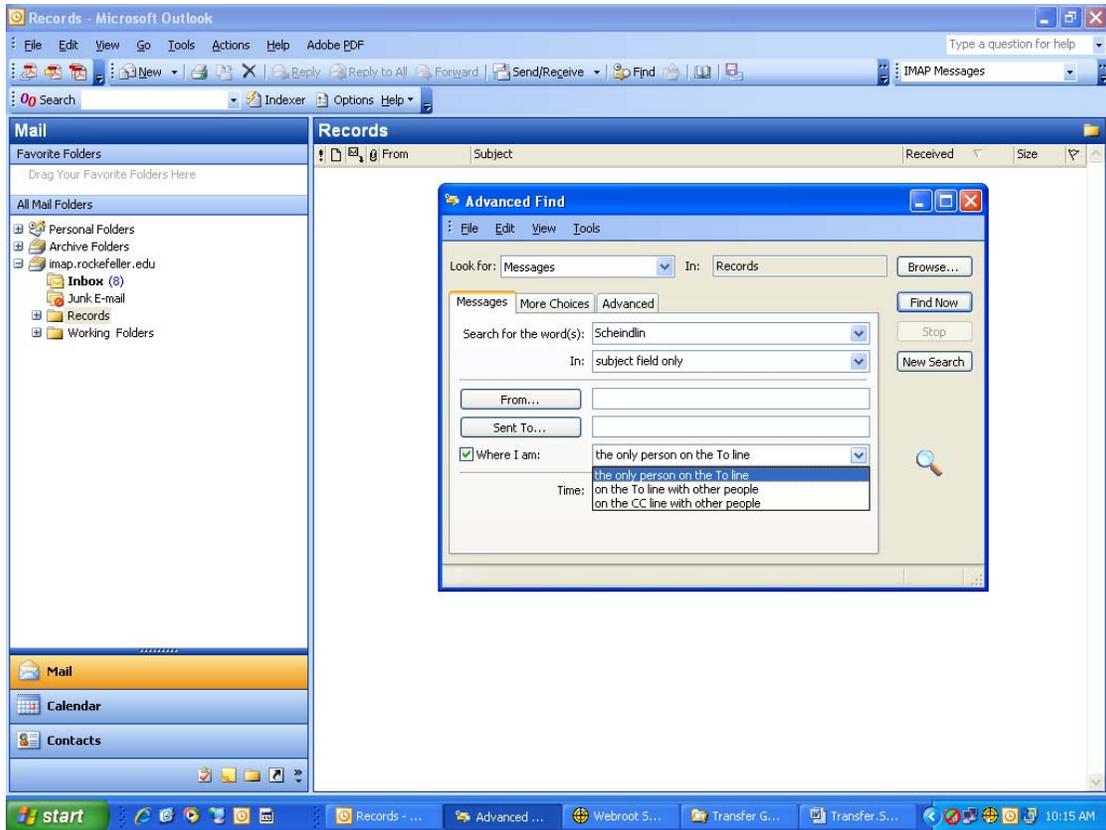
When copying is finished, clear on "Clear" on the Find toolbar to return to the Inbox.

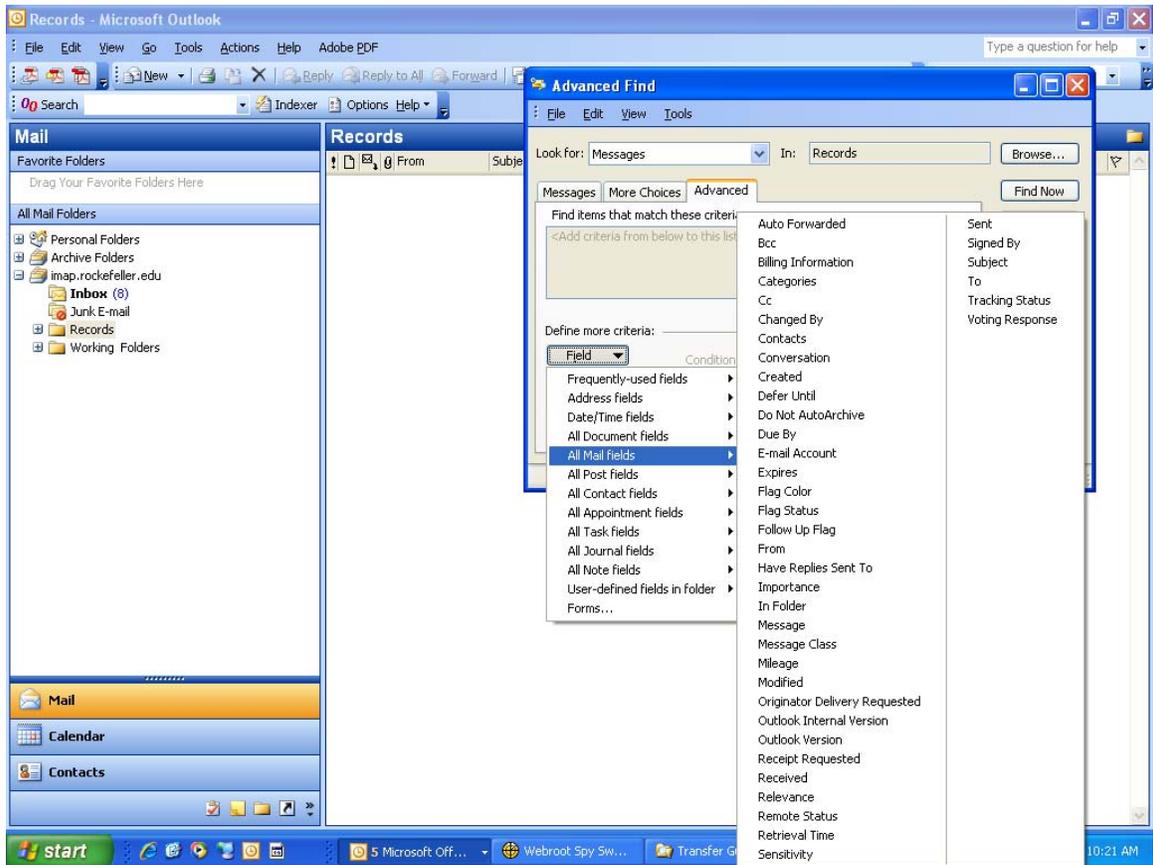
Note: under "All Mail Folders", "imap.xxxxxxxx" folders/files are backed up by the server, so the desired folders could be copied from the server rather than desktop once files have been moved to imap folders.

Advanced searches using a variety of parameters can be done from the “All Mail Folders” point (see page 26) by choosing “Tools”, then “Find”, then “Advanced Find.” Some of the choices appear on the following screen prints. Click on the desired tab – “Messages”, “More Choices”, or “Advanced”, then check the relevant box and/or select from drop down menus to achieve the desired results.









APPENDIX 4

Depositor Transfer Preparedness Survey

(Respond only regarding records you will transfer to the RAC in electronic form.)

1. Estimate in megabytes the total quantity of electronic records generated annually that you expect to eventually transfer to the RAC.

2. What percentage would be in the following categories?

E-mail _____ Database _____ Other (please specify) _____

3. Starting with the earliest year in which your electronic records were created, please advise the following:

Year Created	Type of Format for transfer (e.g. PST, EML)	Method of transfer to RAC (CD, DVD, tape, server, etc.)
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

4. Is your organization following the RAC/CERP E-Mail Guidelines, Transfer Guidelines, and Records Retention Guidelines? If not, please provide a copy of the guidelines and retention schedule you use.

5. How often might you transfer electronic records to the RAC?

6. If you anticipate an initial large transfer consisting of records accumulated over several years, when would you like to make the transfer?

7. How long after creating will you hold electronic records before transfer?

8. On what media and in what temperature and humidity environment will these records be stored between the time they were created and the time they are transferred to the RAC?

9. Will these records be periodically checked for media degradation and data viability, and if so, how often and by whom?

10. What measures will you take to ensure information remains readable prior to transfer to the RAC?

11. How will you ensure that no personal, private, confidential, or spam messages are included in the e-mail you transfer to us?

12. If you do not plan to filter out such non-business messages, are you willing to reimburse the RAC for costs involved in doing so?

13. How will you ensure that e-mail attachments are captured with the e-mail, that they can be located, and that they are readable?

14. Will you segregate material (perhaps in separate folders or on separate media) that is to be closed for a period and mark by opening date, e.g. "Open 1/1/2020"?

15. If not, how do you propose that such material be handled?

16. Who in your organization will have custody of electronic records from the time they are considered non-current to the time they are transferred to the RAC?

17. Who else will have access to electronic records while awaiting transfer?

18. What security precautions will you provide to ensure that records are not tampered with while awaiting transfer?

19. Who in your organization will be responsible for advising the RAC when you are ready to transfer electronic records to us?

20. With respect to e-mail, will you include directory information (e.g. LDAP) with real names associated with e-mail names and mail lists of internal groups?

21. How do you plan to minimize capture of the same e-mail again and again? For example, if you copy John Doe's Inbox "Grants" folder on 3/30/2007, and schedule another ingest on 3/30/2008, will you be capturing only e-mail created between those two dates or will you be capturing all of the original ingest plus the additional?

APPENDIX 5

DoD Compliant Records Management Software⁸

- ▶ Advanced Processing & Imaging, Inc.'s OptiView® Enterprise Content Management v 9.0
- ▶ Autonomy's Meridio Records Management v5.0
- ▶ CA Records Manager v7.5 (SR5) (formerly known as CA MDY FileSurf v7.5 SR5) with Interwoven WorkSite v8.2
- ▶ CA Records Manager v7.5 (SR5) (formerly known as CA MDY FileSurf v7.5 (SR5) with CA Message Manager v11.5.1
- ▶ CA Records Manager v7.5 (SR5) (formerly known as CA MDY FileSurf v7.5 (SR5) with MS SharePoint Server 2007
- ▶ CEXEC eCustodia v2.2 with Microsoft SharePoint Portal Server 2003 and IBM DB2 Records Manager v4.1.2
- ▶ CEXEC eCustodia v3.0 with Microsoft SharePoint Portal Server 2003, IBM DB2 Records Manager v4.1.2, and IBM DB2 Content Manager v8.3
- ▶ DocuWare Version 5.1
- ▶ EMC Documentum Records Manager v6.0
- ▶ EMC Records Activator v5.3–MS SharePoint Integration
- ▶ EMC Documentum Records Manager v5.3 (SP3)
- ▶ e.POWER 6.5 with eDOCS RM 6 (formerly known as Hummingbird DM/RM)
- ▶ IBM FileNet Records Manager 3.7.0 (formerly known as FileNet Records Manager v3.7.0)
- ▶ Innovative Ideas Unlimited, Inc.'s Records Manager Express for Domino Version 8.0
- ▶ Interwoven RecordsManager v6.0
- ▶ Iron Mountain, Inc's, Accutrac XE (formally known as Accutrac Software, Inc.)
- ▶ K Ellis Ltd.'s Secure Records Management 42
- ▶ Laserfiche 8: Records Management Edition
- ▶ Microsoft Office SharePoint Server 2007 with DoD Add–On Pack
- ▶ Objective 7.1

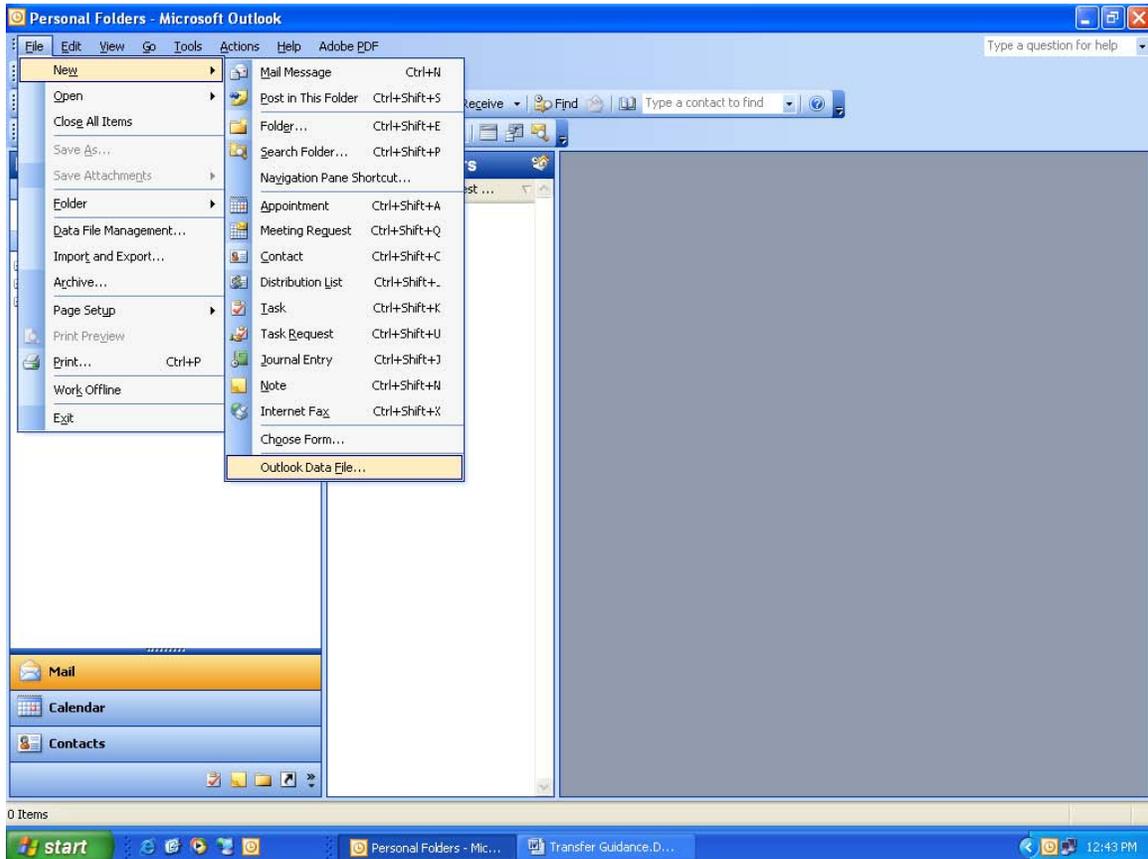
⁸ The United States Department of Defense (DoD) Design Criteria Standard for Electronic Records Management Software Applications, known as DoD 5015.2 is a set of specifications a manufacturer must meet to demonstrate that its product provides the functionality required for DoD records management. DoD certification of a particular software means that it has passed DoD's rigorous design and testing measures. Certification is valid for two years. The United States National Archives & Records Administration (NARA) endorses applications that have been DoD certified.

- ▶ Open Text Corporation, Livelink ECM – Records Management for SAP Solutions v9.6
- ▶ Open Text Corporation's Livelink ECM – MS SharePoint Integration (for SharePoint Server 2003 and Office SharePoint Server 2007)
- ▶ Open Text Corporation's Livelink ECM – Records Management v3.8
- ▶ Open Text Corporation's Livelink ECM – eDOCS RM 6 (formerly known as Hummingbird RM/DM)
- ▶ Oracle USA's Oracle Universal Records Management 10g (formerly known as Stellent Records Management v8)
- ▶ SAP's SAP Public Sector Records Management v2.1
- ▶ Thomson Elite's 3E Records Management v2.1
- ▶ TRIM Context 6, TOWER Software
- ▶ Vignette Records & Documents 7.1
- ▶ Xythos Enterprise Document Manager 6.0

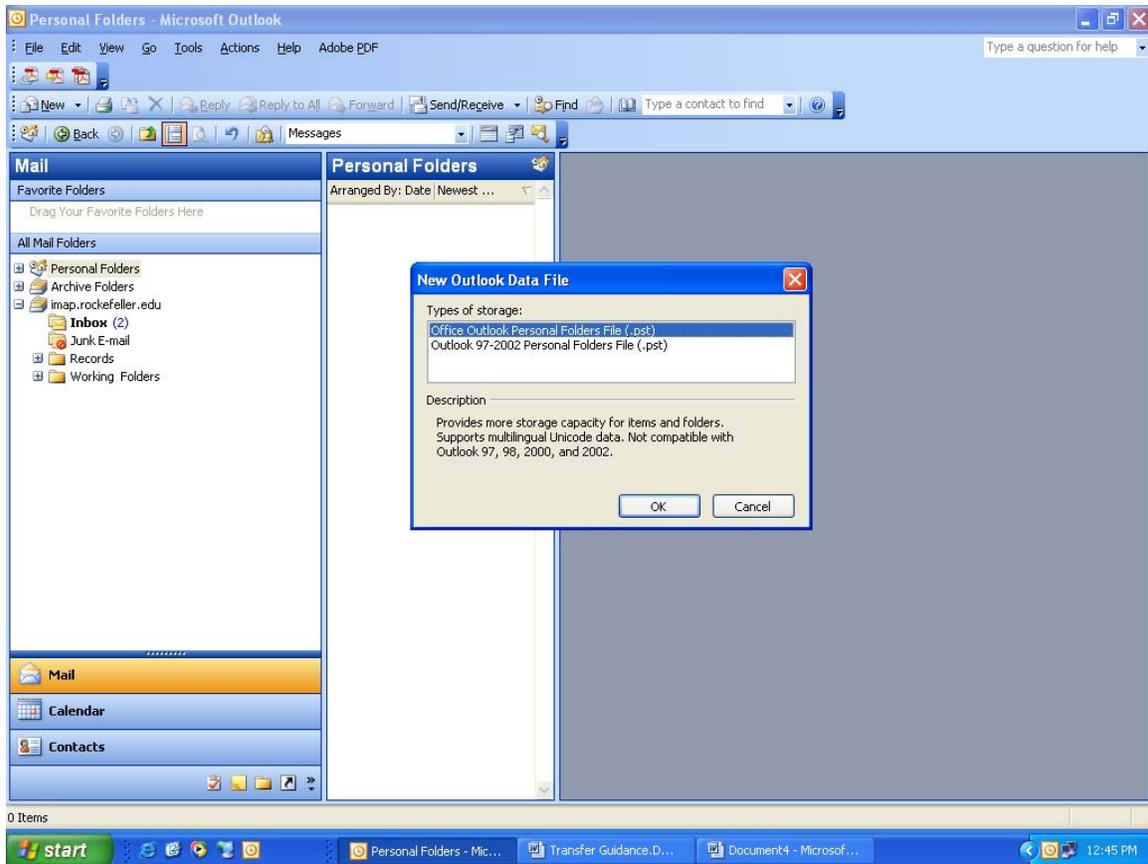
Products listed apply to non-classified records and the list is current as of September 17, 2008. See the DoD website for an updated list:
<http://jitc.fhu.disa.mil/recmgt/register.html> .

APPENDIX 6

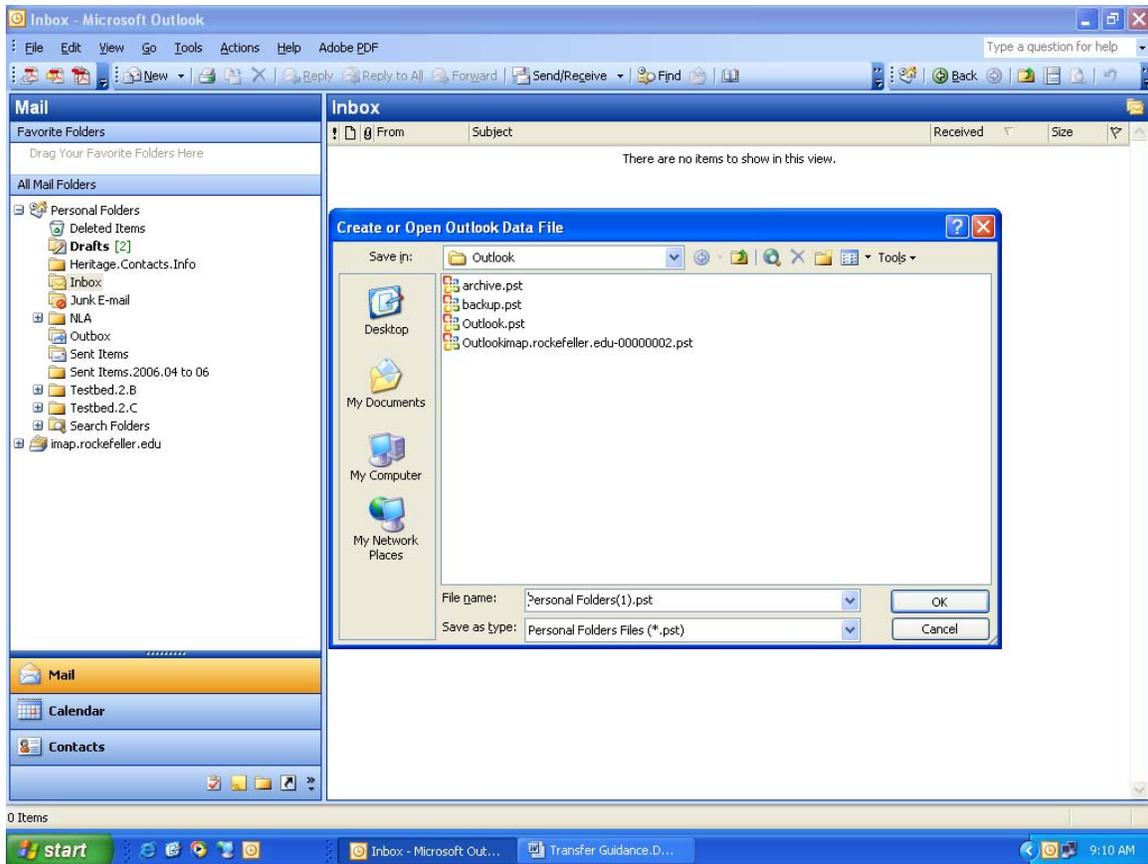
Setting up PST files



With e-mail Inbox open, click on “File” on the toolbar
Click on “Outlook Data File”

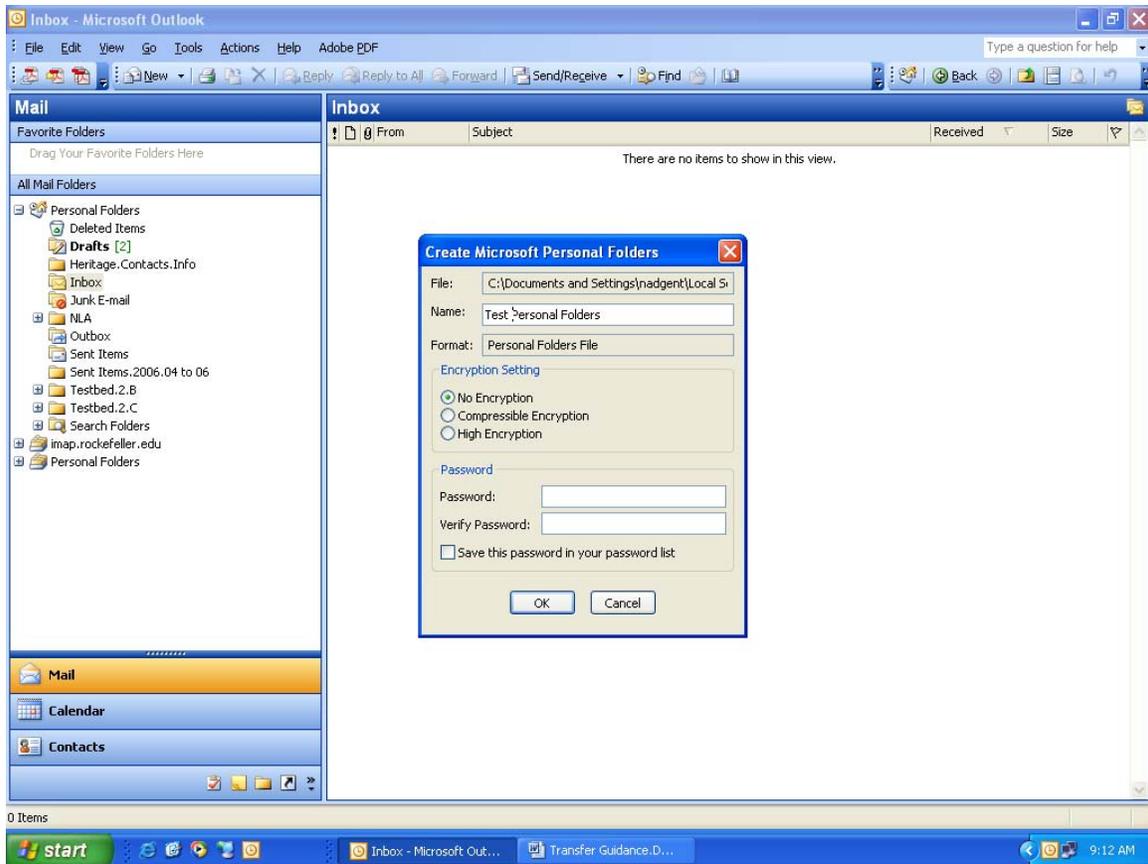


Highlight the appropriate Outlook storage file and click OK



In the “File name” box, change the file folder name unless you want to use the default Personal Folders (1).pst.

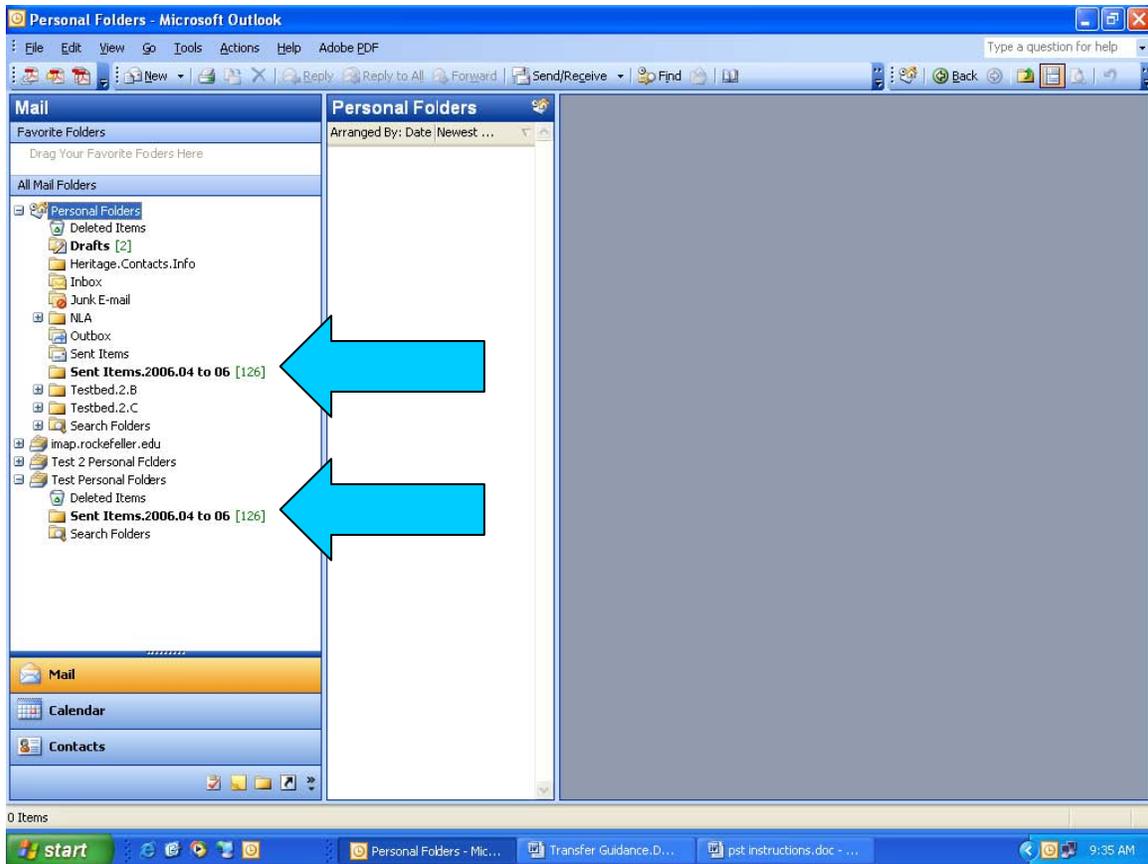
Click OK.



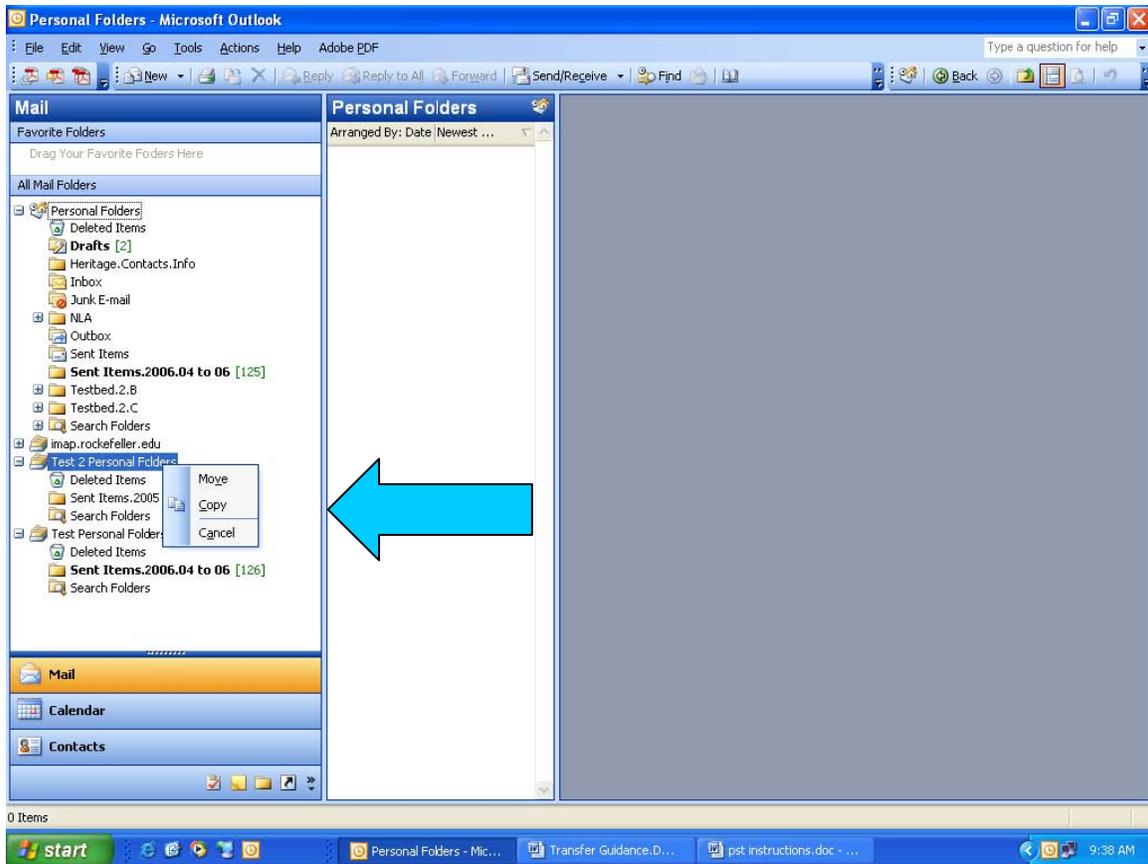
In the “Name” box, type a display name for the .pst folder.

Select any other desired options and click OK.

NOTE: When conducting a .pst conversion on files that will be transferred to the Archive, be sure to select “No Encryption”; if security prior to the transfer is a concern, supply your organization’s Records Manager or the Archive with the encryption password.



Click and drag folder(s) or individual files from existing Personal folders to the new PST folder. In the above example, “Sent Items.2006.04 to 06” was copied to the new PST “Test Personal Folders.” Note that the number of items is the same.



Folders or individual files can be moved or copied to the new .pst folder. Right click on the folder or file you want to move, and drag it to the new location. When the box appears, select “Move” or “Copy.”

APPENDIX 7

Electronic Records Accession and Documentation Form

Collection: _____ **Accession #** _____

RG: _____ **Series:** _____

RG: _____ **Series:** _____

Date(s) Created: _____ **Accession Has Non-Electronic Items:** Y ___ N ___

Container(s) ID: _____ **Container(s) ID:** _____

Media or Ingest Batch ID: _____ **Media or Ingest Batch ID:** _____

Media or Ingest Batch ID: _____ **Media or Ingest Batch ID:** _____

***** Depositor: Please provide an electronic (preferably plain text) and paper list of the files being deposited. Include folder and file names, format and version, size (in bytes), and an individual list of files within compressed/archived files. *****

Depositing Organization: _____

Contact name: _____

Address: _____

E-mail: _____ **Telephone:** _____

Terms (donation, deposit, time period, retention, restrictions): _____

Content (please check all that apply):

Text		Audio	
CAD		Catalogue	
Database		GIS	
Graphics		Images – moving	
Images – still		Numeric dataset	
Software executable		Software source code	
Virtual reality		Website	

Archivist: _____ **Date accessioned:** _____

If the records being deposited are not in their original form, where did the original records reside (e.g. server, hard drive)?

If information on records being deposited has been altered since creation, indicate changes:

Altered by: _____ **Date(s):** _____

If information has been migrated or refreshed since creation, indicate details:

Migrated by: _____ **Date(s):** _____

From format: _____ **To format:** _____

Refreshed by: _____ **Date(s):** _____

From media: _____ **To media:** _____

Copy of verification documentation provided by depositor: ____ **Yes** ____ **No**

If files contain copyrighted material, provide details:

If files contain encrypted material, provide key and details:

Location, physical environment, security of records since creation:

***** Archivist: Complete Electronic Records Transfer, Verification, and Migration Documentation forms *****

AIP # _____ To Digital Repository at _____

Date Sent _____ Date Received Confirmation _____

Media Storage Location for Electronic Records in this accession:

Vault _____ Shelf _____ Unit _____ Box _____ Box _____

Vault _____ Shelf _____ Unit _____ Box _____ Box _____

Vault _____ Shelf _____ Unit _____ Box _____ Box _____

Vault _____ Shelf _____ Unit _____ Box _____ Box _____

Vault _____ Shelf _____ Unit _____ Box _____ Box _____

Vault _____ Shelf _____ Unit _____ Box _____ Box _____

Appendix 9 – Electronic Records Verification Form

Collection	RG				Series		Accession #		AIP #
	Original Source E-mail	Preservation Copy	Virus Scan	Parsed Source	native to .eml	Data Kept / Deleted	User Copy Aid4Mail .eml	User Copy .eml to .mbox	Parsed User Copy
Title/Bundle Name									
Size on disk (KB/MB)									
# folders									
Folder 1									
Size on disk									
# files									
File 1									
Size on disk									
# messages									
# attachments									
# embedded									
File 2									
Size on disk									
File 3									
Size on disk									
File 4									
Size on disk									
Folder 2									
Size on disk									
# files									
File 1									
Size on disk									
# messages									
# attachments									
# embedded									

APPENDIX 11

Glossary*

8.3	The MS-DOS file-naming convention of eight characters followed by a period (.) and three final characters. The three final characters are popularly used as acronyms for the file format of the electronic document. For example, "demo.ppt" is a Microsoft PowerPoint document. PPT would be the ".3" expression, or the acronym for a PowerPoint file.
ASCII	A text file where each character or space is represented by one byte encoded according to the ASCII (American Standard Code for Information Interchange) code.
ASP	Active Server Page. This web page format uses scripting, normally VBScript or JavaScript code in combination with HTML to dynamically generate a complete HTML page for display on the requesting web browser. The complete HTML is not generated until that page is requested by a web browser, allowing webmasters to deliver customized content without dramatically increasing the web content they must manage.
CFM	Cold Fusion template/page. Cold Fusion is a Macromedia web development application used to create dynamic web pages in a fashion similar to the ASP format developed by Microsoft.
CSV	Comma Separated Values. Another name for comma-delimited text format and usually the 8.3 extension value used for this type of format. CSV preserves the data input (not formulae or formatting), allowing a spreadsheet or database to be recreated later.
DPI	Dots per inch. A means of expressing the amount of information recorded in a digital image correlating to the resolution of the image.
JPEG/JPG	JPEG is a lossy compression technique for color images developed by the Joint Photographic Experts Group. File sizes can be reduced, but with a loss in detail. JPG is an alternate representation of JPEG.

PDF	Portable Document Format developed by Adobe Systems.
RGB	Red, Green, Blue components of a color TIFF image
RTF	Rich Text Format. A format standard which embeds basic formatting instructions in an essentially ASCII document. Margins, font style, indentation and other formatting instructions are supported.
SWF	Shockwave file format used by Macromedia's Flash player application. An increasingly popular plug-in, or supplemental application, used with web browsers. Such a file is commonly referred as a Flash component.
TIFF	Tagged Image File Format. Very popular format for storing bit-mapped images. Supports black-and-white, grayscale, and color images. Orders the bytes of the image file in either Intel (PC) order or Macintosh order.
Unicode	A character encoding standard developed by the Unicode Consortium. By using more than one byte to represent each character, Unicode enables almost all of the written languages in the world to be represented by using a single character set.
URL	Universal Resource Locator. The "address" of an Internet-accessible document. Most frequently begins with "http://..." but also includes "ftp://..." and "telnet://..." Unfortunately, the longevity of a given URL has been documented to be only six months, on the average, in today's Internet culture.
XHTML	Extensible Hypertext Markup Language. This information standard essentially expresses HTML code in an XML syntax. XHTML 1.0 has been recognized by the Internet-related vendors as the successor to HTML 4.0 and is the equivalent of the most recently adopted HTML 4.1 protocol.
XML	Extensible Markup Language. A flexible text format derived from the Standard Generalized Markup Language (SGML) to meet the challenges of large-scale electronic publishing. Its uses have since spread into database environments as well.

*Based on Smithsonian Institution Archives Glossary. See <http://siarchives.si.edu/cerp> for a more comprehensive CERP Glossary.