



Australian Government

Department of Education, Employment and Workplace Relations

PSPPOL405A Implement e-correspondence policies

Revision Number: 3

PSPPOL405A Implement e-correspondence policies

Modification History

Release	TP Version	Comments
3	PSP12V1	Unit descriptor edited.
2	PSP04V4.2.	Layout adjusted. No changes to content.
1	PSP04V4.1	Primary release.

Unit Descriptor

This unit covers the competencies required to send and receive email correspondence (e-correspondence) via the internet, intranets or extranets. It also covers setting up and maintaining electronic software; maintaining and managing individual electronic mail (email) mailing lists and address books; implementing email policy; and adhering to organisational protocols and practices for email.

In practice, implementing e-correspondence policies overlaps with other generalist and specialist work activities, such as upholding and supporting the values and principles of public service, applying government processes and using advanced workplace communication strategies.

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement.

Application of the Unit

This unit applies to organisations that have electronic mail systems which are integral to their business processes, and need to ensure that incoming and outgoing mail is tracked and stored with integrity.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.

Performance criteria describe the performance needed to demonstrate achievement of the element. Where ***bold italicised*** text is used, further information is detailed in the range statement. Assessment of performance is to be consistent with the evidence guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. Set up and send electronic mail	1.1. <i>Software for sending and protecting email</i> is <i>set up</i> and maintained according to <i>organisational requirements</i>. 1.2. Messages are prepared according to <i>organisational protocols</i> for language, tone and format. 1.3. Content, structure and recipient addresses for electronic mail are <i>checked for accuracy</i> and <i>attachments identified and prepared</i> according to organisational and service provider requirements. 1.4. Records and/or copies of outgoing electronic mail are maintained according to organisational requirements. 1.5. Electronic mail is <i>dispatched</i> according to organisational requirements and within required timeframes.
2. Implement procedures to receive electronic mail	2.1. Procedures are implemented to ensure incoming electronic mail is recorded and/or copied according to organisational requirements. 2.2. Urgent, confidential and personal mail is identified and forwarded according to organisational requirements. 2.3. Procedures to identify <i>suspicious or potentially dangerous electronic mail</i> are implemented according to organisational requirements. 2.4. Electronic mail is checked for completeness, and opened or forwarded according to organisational policy and procedures relating to confidentiality and privacy. 2.5. <i>Returned email is dealt with</i> according to organisational policies and procedures.
3. Manage electronic mail	3.1. Security levels and/or filters are set for incoming electronic mail according to organisational requirements. 3.2. Individual mailboxes are created and maintained according to organisational requirements. 3.3. Inboxes are emptied and electronic mail is archived or permanently deleted according to organisational requirements. 3.4. Electronic mail and/or attachments are <i>stored</i> according to organisational requirements. 3.5. Electronic <i>mailing lists</i> are prepared and maintained according to organisational requirements. 3.6. Mailing lists are imported and exported between software applications where required and according to organisational requirements.

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- computer technology skills to manage and maintain email
- literacy skills to:
 - compose and check accuracy of messages
 - follow policies and procedures
- communication skills to refer information to management or other staff, especially in dealing with suspicious or potentially dangerous electronic mail
- interpersonal skills to provide information to people from a range of social, cultural and ethnic backgrounds and physical and mental abilities

Required knowledge

- relevant legislation from all levels of government that affects e-business operation, especially in regard to OHS and environmental issues, equal employment opportunity, industrial relations and anti-discrimination
- organisational policies and procedures relating to electronic mail
- service provider requirements, especially with regard to email attachments
- set up and maintenance procedures for electronic software
- naming protocols for email addresses
- electronic file handling, including saving, copying, moving and deleting
- security levels for receiving electronic mail
- OHS requirements for working with computer technology

Evidence Guide

The Evidence Guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment Competency must be demonstrated in sending and receiving email correspondence via the internet, intranets or extranets, setting up and maintaining electronic software, individual electronic mailing lists and address books, implementing email policy and adhering to organisational practices for email

Critical aspects for assessment and evidence required to demonstrate competency in this unit

Assessment must confirm the ability to:

- send a range of e-correspondence that meets communication requirements and complies with organisational protocols for content, accuracy and timeliness
- securely receive and process e-correspondence according to organisational requirements
- sort, file, delete and archive e-correspondence according to organisational requirements.

Consistency in performance

Competency should be demonstrated by managing incoming and outgoing e-correspondence, covering a range of types of communication over an extended period.

Context of and specific resources for assessment

Assessment must comply with:

- organisational client management and health and safety procedures
- applicable regulations and codes.

Access may be required to:

- a simulated work environment
- organisational policies and procedures
- relevant legislation, case law and guidelines.

Guidance information for assessment

The following assessment methods are suggested:

- oral questioning about software functions, security measures and communication protocols
- feedback from peers and/or supervisor that the candidate consistently applies relevant workplace protocols and procedures
- review of e-correspondence sent by the candidate and filing and archiving of correspondence conducted by the candidate or reports of performance.

In all cases, practical assessment should be supported by questions to assess underpinning knowledge and those aspects of competency that are difficult to assess directly. Questioning techniques should suit the language and literacy levels of the candidate.

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Software for sending and protecting email may include:

- virus protection
- firewalls
- encryption

Set up may include:

- set up procedures, especially in non-networked situations where there is no system administrator
- creating folders
- procedures for general housekeeping, such as:
 - archiving files
 - emptying temporary internet folders and cookies, etc

Organisational requirements:

- may include legislation, codes and national standards relevant to the workplace, including:
 - award and enterprise agreements
 - commonwealth, state and territory legislative requirements especially in regard to OHS
 - industry codes of practice
- must include:
 - copyright laws
 - defamation laws
 - privacy legislation
 - Spam Act
 - intellectual property and confidentiality requirements
 - legal, regulatory and organisational policies affecting e-business
 - codes of conduct

Organisational protocols may include:

- net etiquette (netiquette), including:
 - observing codes of conduct or codes of practice with regard to privacy and confidentiality
 - following accepted (not mandated) rules for being a good net citizen (netizen)
 - responding in a professional manner
 - adjusting to the style and tone of discussion

groups

- respecting others' time and bandwidth
- maintaining consistent presentation standards of correspondence, including spelling and grammar
- sharing knowledge
- net ethics (nethics), including behaviour on the internet, such as respecting copyright and intellectual property rights

Checked for accuracy
should include:

- clarity of intended meaning
- spelling
- grammar
- punctuation

Identifying and preparing attachments
may include:

- dealing with large attachments especially picture files
- considering limitations when sending large files
- checking maximum file size acceptable to an enquirer's internet service provider
- separating large documents into a number of files
- compressing files
- running and handling self-executable files
- uploading to third-party online storage providers

Dispatched may include:

- single receiver
- group email
- carbon copies
- blind carbon copies
- email bulletin board or discussion list

Suspicious or potentially dangerous email may include:

- unsolicited mail containing viruses or malware
- spam
- mail where sender is unknown and subject line is enticing and/or personal
- attachments
- particular file extensions

Dealing with returned email may include:

- checking email address
- checking size of attachments
- re-sending
- sending message by other means, e.g. facsimile or post
- telephoning addressee
- removing from mailing lists

Stored may include:

- within electronic mail application software
- specialised record keeping, spreadsheet or database software
- paper-based filing system
- third-party online service provider
- cloud computing services

Mailing lists may include:

- electronic address books
- database or spreadsheet records

- word processing tables or data files

Unit Sector(s)

Competency field

Policy.