ICAICT108A Use digital literacy skills to access the internet

Release: 1

ICAICT108A Use digital literacy skills to access the internet

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to safely and securely use the internet to undertake basic interactive communication.

It involves a working knowledge of current industry standard technologies and the ability to apply these technologies to a number of digital literacy situations.

Application of the Unit

This unit applies to individuals who locate, organise, understand, evaluate and analyse information using digital technology in the areas of entertainment, communication, internet searching, online participation, networking and commercial transactions.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
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 required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.*

Elements and Performance Criteria

1. Operate hardware at a basic level	1.1. Identify *hardware components* required to connect to the internet
	1.2 Set up and check physical *connectivity of devices*
	1.3 Use hardware components in an *OHS compliant* way
2. Ensure safe and secure online access	2.1 Connect and access *relevant internet sites*
	2.2 Provide an appropriate level of personal information to maintain privacy and security
	2.3 Comply with *copyright and intellectual property* legislation
	2.4 Ensure an understanding of *socially responsible behaviour*
	2.5 Assess the legitimacy of online requests to make an informed decision
	2.6 Interpret and respond to security notifications that display due to *browser software security* settings or internet use
	2.7 Assess email status and determine *email security*
	2.8 Provide appropriate information to manage *digital footprint*
	2.9 Assess the security of payments
	2.10 Back up data as required through downloading to an *external backup device*
3. Research and analyse online information	3.1 Identify and use search engines to access *relevant internet sites*
	3.2 Search and find relevant information or content
	3.3 Refine search to increase relevance of information or content
	3.4 Navigate a website to access the information or content required
	3.5 Assess payment requirements to make sound financial decisions
	3.6 Analyse the usefulness and accuracy of located information
4. Make transactions and participate online	4.1 Create, register, manage and secure an account
	4.2 Observe appropriate user protocol online
	4.3 Make *secure transactions and identify methods of internet fraud*
	4.4 Identify and invite relevant friends, groups and pages to own website
5. Use applications and	5.1 Use *basic application* skills

manipulate files	5.2 Incorporate attachments to documents
	5.3 Back up files to ***external storage devices***
	5.4 Upload relevant components to a website
	5.5 Download pictures and videos to an external device

5.2 Incorporate attachments to documents

Required Skills and Knowledge

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

Required skills

- communication skills to:
  - communicate with peers and supervisors
  - seek assistance and expert advice
  - undertake online transactions
- keyboarding skills to enter text into web browsers and email applications
- literacy skills to:
  - compose email messages
  - read and interpret basic online content
  - read and write at a basic level
- problem-solving skills to address common operational problems when using web browsers
- research skills to locate varied sources of information online
- technical skills to:
  - operate a digital device
  - use email applications
  - use internet search functions
  - use peripheral hardware.

Required knowledge

- types and basic components of hardware and storage devices
- types of online entertainment
- types of online communication
- basic research and analysis theory
- basic copyright legislation
- digital footprint and basic security, safety and legal issues
- OHS, including basic ergonomics of keyboard and computer use
- types of online participation
- types of online transactions
- device interface
- desk top icons
- basic principles of web browser search engines
- internet
- features of basic applications.

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	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	Evidence of the ability to: • connect to and access the internet • send and receive emails • secure internet access and email communications • use search tools to locate information or content • research and select appropriate websites • undertake online interactions • make an informed assessment of the accuracy, currency, authority and reliability of the site and information located.
Context of and specific resources for assessment	Assessment must ensure access to: • hardware with internet assess • search engines currently used in industry. Where applicable, physical resources should include equipment modified for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • oral or written questioning to assess candidate's knowledge of internet access requirements, email features and security or safety issues • direct observation of candidate accessing the internet, using email, and searching and interacting with consumer sites using correct netiquette • direct observation of candidate undertaking online interactions • review of search results prepared by candidate, including assessment of the accuracy, currency and reliability of the site and information located.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate. Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the

	work being performed.
	Indigenous people and other people from a non-English speaking background may need additional support.
	In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

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.

Hardware components may include:	• Bluetooth device • fax and modem • keyboard • laptop • mobile phone • monitor • mouse • multimedia kit • personal computer • personal digital assistant (PDA), such as palmtop • printer • scanner • speaker • tape cartridge • universal serial bus (USB) device • wi-fi router.
Connectivity of devices may include:	• Bluetooth device • hard drive • keyboard • laptop • mobile phone • modem • mouse • multimedia kit • pen • PDA, such as palmtop • printer • scanner • speaker • tape cartridge • touch pad • USB device • wireless fidelity (wi-fi) router • headphone and microphone

	• web camera.

OHS compliant may include:	• electrical safety
	• ergonomics in the workplace:
	    • correct posture
	    • style and adjustment of chair
	    • type of desk
	    • type of monitor
	    • working position
	    • length of time in front of computer
	    • lighting level
	    • placement of light fittings
	    • repetitive strain injury (RSI) prevention
	    • safe lifting methods
	    • ventilation
	• social problems associated with internet and computing addictions.

Relevant internet sites may be used for:	• entertainment:
	    • internet TV
	    • games
	    • videos and podcasts
	    • music
	• communication:
	    • email
	    • Skype
	    • instant messaging
	• finding using and storing information:
	    • searching to enhance personal knowledge and interest and to make informed decisions
	    • participating online
	    • online consultation, forum and discussion
	    • posting photos and videos
	    • applying for jobs
	• networking and collaboration:
	    • social networking
	    • online dating
	    • transactions
	• banking
	• government services, including registrations
	• buying and selling:
	    • travel

	• paying bills • trading shares.
Copyright and intellectual property may relate to:	• copyright infringement legislation • electronic resources usage policies • ethical use of digital technologies • ethical decision making when facing inappropriate acts of technology use.
Socially responsible behaviour may relate to:	• not using obscene, profane, lewd, vulgar, rude, inflammatory or threatening language • not publishing information that, if acted upon, could cause damage to property or persons, nor publish deliberately false or defamatory information about a person or organisation • not engaging in personal attacks, including prejudicial or discriminatory attacks • not harassing, distressing or annoying another person • not accessing material that is profane, obscene or pornographic, that promotes illegal acts, or that advocates violence or discrimination • not sending inappropriate emails • taking responsibility for protecting personal information and not revealing personal information, including names, addresses, photographs, credit card details and telephone numbers.
Browser software security may include:	• application enabling • cookie handling • pop-up blocking • privacy levels • security zones • trusted sites.

Email security may relate to:	• taking steps to restrict:
	  • malware
	  • phishing
	  • spam
	  • scams.

Digital footprint may include:	• tracking of internet usage, such as:
	  • system login and logouts
	  • visits to a web page
	  • accessed or created files
	  • email messages
	  • chat messages.

External backup	• DVDs

devices may include:	- memory cards - memory sticks - USB drives - hard drives.
Secure transactions may include:	- web browser - secure socket layer (SSL) - security verified sites - digital certificates - VeriSign - online payment services - PayPal - stored-value cards - smart cards - point-of-sale devices - digital cash - e-wallets.
Methods of internet fraud may include:	- invalid internet sites - credit card fraud - identification theft - impulse buying strategies.
Basic applications may include:	- databases - email - internet browsers - spreadsheets - system browsers - word processing.

Unit Sector(s)

General ICT