



Australian Government

Department of Education, Employment and Workplace Relations

ICAICT418A Contribute to copyright, ethics and privacy in an IT environment

Release: 1

ICAICT418A Contribute to copyright, ethics and privacy in an IT environment

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to maintain professional and ethical conduct as well as to ensure that personal information of stakeholders is handled in a confidential and professional manner when dealing with stakeholders in an information technology (IT) environment.

Application of the Unit

This unit applies to IT personnel who are required to gather information to determine the organisation's code of ethics, and protect and maintain privacy policies and system security.

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
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>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.</i>

Elements and Performance Criteria

1. Protect intellectual property	1.1 Identify current legislation and standards relating to intellectual property and copyright 1.2 Investigate current organisational copyright policy 1.3 Adhere to organisational policy and current legislation in work practices
2. Contribute to copyright policy	2.1 Contribute to the creation or updating of the organisation's copyright policy and procedures to align with legislation and industry standards 2.2 Distribute new or revised policy and procedures to stakeholders
3. Protect rights of stakeholders	3.1 Identify and document the relevance of legislation and standards to organisational outcomes 3.2 Investigate and review organisational privacy policy and procedures 3.3 Investigate and review organisational code of ethics 3.4 Determine the integrity, confidentiality, security and availability of information as required by organisational policy 3.5 Maintain confidentiality and proprietary rights of stakeholder interests
4. Contribute to privacy policy	4.1 Contribute to the creation or updating of the organisational privacy policy and procedures to align with privacy legislation 4.2 Distribute new or revised policy and procedures to stakeholders 4.3 Implement new work procedures and collect feedback from stakeholders 4.4 Ensure the integrity, confidentiality, security and availability of information as required by organisational policy
5. Maintain privacy policy	5.1 Review work practices to ensure application of privacy policy and procedures 5.2 Maintain the integrity, confidentiality, and availability of information as required by organisational privacy policy 5.3 Review work practices to ensure system security according to organisational privacy policy
6. Contribute to creation of ethics code	6.1 Assist in developing or updating a code of ethics to align with legislation and standards for the organisation 6.2 Distribute the new ethics code to stakeholders and collect

	feedback 6.3 Implement new ethical work procedures and collect feedback 6.4 Review ethical work practices and feedback to ensure application of the code
7. Maintain ethics code	7.1 Perform regular checks to ensure stakeholders understand and are continuing to apply the code of ethics in the workplace 7.2 Establish a review and grievance procedure to enable confidential reporting of any ethical issues 7.3 Interview and regularly follow up with stakeholders to ensure they are receiving consistent and appropriate service in dealing with the code of ethics

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on ethical and privacy, operational and business-related matters
- learning skills to update personal ethical and privacy knowledge through professional development
- literacy skills to apply standards and legislation to policy and procedure development and monitoring
- planning and organisational skills to plan, prioritise and monitor own work
- research skills to gain and maintain current industry privacy and ethical information
- technical skills to perform application and system security and storage management.

Required knowledge

- Australian Computer Society Code of Ethics
- federal and state or territory legislation and policy relevant to an IT environment relating to:
 - access and equity
 - copyright and intellectual property
 - OHS
 - privacy
- organisational communication processes and procedures
- organisational requirements for customer service
- server operating systems
- system security procedures.

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: - analyse legislation and standards relating to professional conduct and privacy in the IT industry - contribute to the development of a code of ethics and monitor the workplace to ensure code of ethics is being applied and is appropriate - contribute to the development of a privacy policy and monitor the workplace to ensure the policy is being applied and is appropriate.
Context of and specific resources for assessment	Assessment must ensure access to: - relevant organisational policies, legislation and standards documentation - industry codes of practice - appropriate learning and assessment support when required. 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: - direct observation of candidate monitoring continuity of computing services and information flow to ensure the protection of stakeholder interests - review of candidate's documented code of ethics and privacy policy - verbal or written questioning to assess candidate's provision of some leadership and guidance to others in the implementation of ethical conduct in business relationships - verbal or written questioning to assess candidate's ability to provide guidance to others in the operation and management of privacy policies in business relationships.
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.

Legislation and standards may include:	• access and equity • confidentiality requirements • copyright laws • defamation laws • industry codes of practice, such as Australian Computer Society Code of Ethics • industry standards • intellectual property • international standards • International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Australian Standards (AS) • legal and regulatory policies affecting ebusiness • OECD Guidelines for Consumer Protection in the Context of Electronic Commerce • OHS • organisational standards • privacy legislation • project standards.
Privacy policy may include:	• access of personal information • disclosure of personal information • gathering of personal information • organisation standards and practices • quality of personal information • security of personal information • sensitivity of personal information • storage of personal information • use of personal information.
Stakeholders may include:	• authorised business representative • colleagues • individuals • internal departments • internal employees • external organisations

	• clients • project manager • supervisor • users.
--	---

Unit Sector(s)

General ICT