Title	**Use digital tools securely, safely, ethically and legally**		
Level	**2**	**Credits**	**5**

Purpose	People credited with this unit standard are able to: demonstrate knowledge of relevant legal requirements and ethical responsibilities when using digital tools; and identify risks, procedures and solutions to implement and maintain basic digital safety and security when using digital tools in a home, work or study context. This unit standard has been developed primarily for assessment within programmes leading to the New Zealand Certificate in Computing (Foundation User) (Level 2) [Ref: 4132].

Classification	Computing > Generic Computing

Available grade	Achieved

Guidance Information

1 Assessment, where applicable, will be conducted in and for the context of real or realistic situations and/or settings, and be relevant to current and/or emerging practice. The assessor may gather evidence over time from a range of scenarios rather than using one assessment where the learner has to demonstrate all of the required skills. For assessment purposes this standard is a practical demonstration of knowledge. Oral or written responses may be used to clarify knowledge.

2 The specified issues will be provided to the learner, and may be in the form of scenarios. The specified issues/scenarios provided will enable learners to demonstrate awareness and knowledge of relevant legal requirements when using digital devices and will provide requirements against which success or otherwise can be evaluated. The specified issues/scenarios must be of sufficient complexity to provide scope for the assessment evidence and to meet the intended purpose.

3 Definitions
Anti-malware is the generic term used to describe the prevention, detection, and removal of malicious software such as virus, Trojans, spyware and other harmful programs.
Basic security risks refer to unauthorised access, malware, power failure, natural disaster, data corruption, hardware failure, network access.
Digital devices refer to an electronic computing device that can receive, store, process or send digital information, such as computers (desktop or laptop), tablets, smartphones or other emerging digital technologies.

Digital tools may be both hardware (digital devices) and software (applications and programs).
Malware refers to a type of malicious code that includes viruses, Trojans, worms, backdoor, spyware and other harmful programs.
Security measures and solutions refer to log-off, shut-down; anti-malware software, firewalls; browser settings, passwords, access control, read only files, physical security/locking; back-up and restore techniques; frequency of saving; UPS or surge protector; personal network protection.
Security risks in this standard refer to the transparency and accessibility of information and prevention through maintaining basic security requirements to minimise harm, in a home, work or study context.

4 Legislation relevant to this unit standard includes but is not limited to the:
Copyright Act 1994
Copyright (New Technologies) Amendment Act 2008
Crimes Act 1961
Harmful Digital Communications Act 2015
Health and Safety at Work Act 2015
Privacy Act 2020
Unsolicited Electronic Messages Act 2007
and any subsequent amendments.
Current legislation and regulations can be accessed at http://legislation.govt.nz.

5 Reference
ACC5637 Guidelines for Using Computers - Preventing and managing discomfort, pain and injury. Accident Compensation Corporation - Department of Labour, 2010, available from Worksafe New Zealand, at http://www.business.govt.nz/worksafe/information-guidance/all-guidance-items/guidelines-for-using-computers.

Outcomes and performance criteria

Outcome 1

Demonstrate knowledge of relevant legal requirements and ethical responsibilities when using digital tools.

Performance criteria

1.1 Legislation and guidelines relevant to using digital tools are identified and described in relation to a given range of specified issues.

Range includes but is not limited to – guidelines for using computers; privacy; copyright; health and safety; software licensing, cyber safety.

1.2 Ethical responsibilities when using digital tools are identified.

Range includes – information privacy; copyright; software licensing.

Outcome 2

Identify risks, procedures and solutions to implement and maintain basic digital safety and security when using digital tools in a home, work or study context.

Performance criteria

2.1 Basic security risks when using digital tools are identified and described in terms of their potential impact on the data or system.

Range may include but is not limited to – unauthorised access, malware, power failure, natural disaster, data corruption, hardware failure, network access;
evidence of at least five basic security risks is required.

2.2 Procedures and solutions to implement basic security and maintain basic digital safety in a home, work or study context when using digital tools are identified and described.

Range security measures and solutions may include but are not limited to – log-off, shut-down; anti-malware software, firewalls; browser settings, passwords, access control, read only files, physical security/locking; back-up and restore techniques; frequency of saving; UPS or surge protector; personal network protection;
evidence of at least five security measures or solutions is required.

2.3 Basic digital safety and security measures and solutions when using digital tools are implemented and maintained in a home, work or study context.

Range security measures and solutions may include but are not limited to – log-off, shut-down; anti-malware software, firewalls; browser settings, passwords, access control, read only files, physical security/locking; back-up and restore techniques; frequency of saving; UPS or surge protector; personal network protection;
evidence of five security measures or solutions is required.

Replacement information	This unit standard replaced unit standard 29783.

Planned review date	31 December 2026

Status information and last date for assessment for superseded versions

Process	Version	Date	Last Date for Assessment
Registration	1	26 May 2022	N/A

Consent and Moderation Requirements (CMR) reference	0099

This CMR can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.

Comments on this unit standard

Please contact Toi Mai Workforce Development Council qualifications@toimai.nz if you wish to suggest changes to the content of this unit standard.