

Assessor Guide

Unit Standard 25662 – Version 1

Use digital communications technologies

Level 2 – 3 Credits

Introduction

The tasks in the Learning Assessment Guide for unit standard 25662 are designed to show that the learner can:

- Explain the use of digital communication technologies (DCTs).
- Use DCTs.
- Manage DCTs.

The Learning Assessment Guide is made up of:

- Task(s) for the learner to complete
- Manager or Team Leader Verification/Observation Feedback form.
- Assessment Guide that the assessor will use to assess the learner's competence.

For your information, a copy of the unit standard is attached to the end of this Assessor Guide.

Special notes relating to this unit standard:

1. *Digital communication technologies (DCTs)* – digital tools to enable interaction and communication for example:
 - email
 - Short Message Service (SMS) eg texts
 - Multimedia Message Service (MMS)
 - Voice-over-Internet protocol (VoIP)
 - social software
 - blog
 - wiki
 - forum
 - usenet
 - mailing lists
 - websites

Recognised conventions – usually accepted and/or documented practice of the organisation or workplace eg use of capitals, abbreviations, acronyms, naming, use of hyperlinks, appropriateness of content, referencing of source material.

2. Legislation you may need to consider includes:
 - Copyright Act 1994
 - Health and Safety in Employment Act 1992
 - Privacy Act 1993
 - Unsolicited Electronic Messages Act 2007 and their subsequent amendments.

Assessment Task One – Element 1

Introduction

The purpose of this task is to assess the learner's ability to explain the use of digital communications technologies.

Instructions

The learner must answer a set of questions designed to assess their understanding of DCTs. They may answer in writing or orally. If they choose to answer orally please make a record of their answers for moderation purposes. You may also wish to ask further questions to check understanding or for sufficiency of evidence.

Model answers are provided below as a guide. These answers are not definitive – the learner may raise other points or issues. Please note that as this is a level 2 unit standard, a high level of technical detail is not required.

The evidence required for assessment task one will include:

- Answers to all questions.
- Assessor's notes where relevant.

Question One

Consider the following types of digital communication technologies (DCTs). Choose **three** and give a brief explanation of what they are used for, including the technology used e.g. hardware or software technology.

DCT	Technology used
Email	<i>Used to send electronic messages and to which files or documents can be attached. Requires computer or cellphone with internet or Wifi connection and an email application such as Thunderbird, Outlook etc.</i>
SMS	<i>Used to send short messages over the mobile phone network – requires a phone connected to mobile network.</i>
MMS	<i>This enables a person to send messages over the mobile network that include video and graphics. Technology required is as above but with a WAP (wireless application protocol) browser to handle the video and graphics.</i>
VoiP	<i>This enables the user to use the internet to make phone calls. It also enables the user to see the other person by use of a webcam. VoIP requires a computer with a broadband connection and a VoIP software application such as Skype. A Webcam is required for video.</i>
Social software	<i>Examples include Blogs and Wikis. Social software is used as a means of communication that can be viewed by a number of people over the internet. You need a computer with an internet connection, and a webcam or the ability to upload video and photos if you wish to incorporate these. The software includes such sites as You Tube, Facebook, MySpace . In business, Enterprise 2.0 can be used with corporate intranets as a means of organisational communication and organisation.</i>

DCT	Technology used
Blog	<i>Blogs are similar to an on-line diary or journal. You need a computer with an internet connection and web browser, and subscription to a website that allows blogs.</i>
Wiki	<i>This is software that enables web pages to be created and edited collaboratively using a common web browser. A computer with internet connection is required.</i>
Forum	<i>Forums use web sites as a means of communication with others on specific topics. They are often used to ask questions or discuss ideas. A PC with an internet connection is required.</i>
Usenet	<i>A loose connection of internet servers used as an internet discussion board. The messages are public and generally not moderated. Users need a computer and connection to the internet.</i>
Mailing lists	<i>Lists of clients with their addresses can be held on a database or on an email contact list. They can be then used to mass-mail information. A computer with word processing software and a printer, or internet connection and an email client are required,.</i>
Websites	<i>A computer with an internet connection is required, with web design software such Frontpage to create the site, and a web browser such as Firefox or Internet Explorer to view it. The site is hosted on a server, usually the Internet Service Provider's server is used, however large organisations may host their own.</i>

Question Two

There are situations where the use of DCTs are inappropriate. For each of the first four situations give an example of such a situation. Explain why it would be inappropriate to use a DCT from the standpoint of your responsibility of a user and protocol of the organisation or DCT. The 'other' situation (optional) may be used to address a situation important to you that is not covered by the previous four.

	Example	Why DCT inappropriate
Personal	<i>When something sensitive needs to be discussed.</i>	<i>DCTs are an impersonal method of communication. Even over a video link, it is not always possible to pick up nuances in the voice or facial expression.</i>
Business	<i>A conversation with a client that may require some negotiation, or is sensitive.</i>	<i>As for personal, sometimes a face-to-face meeting is better. The client feels they are more valued if you take the time to meet with them personally.</i>
Time	<i>When something needs to be negotiated or discussed in depth.</i>	<i>It is quicker to have a long dialogue verbally.</i>
Cost	<i>A personal call on the company mobile using MMS.</i>	<i>This costs the business – mobile calls can be expensive, especially streaming video.</i>
Other (optional) please identify		

Question Three

There are various ethical and legal considerations surrounding the use of digital communication technologies. These issues may also constitute a threat to the DCT. Choose **two** of the issues below and explain their characteristics, effects, and the methods of prevention and response to the issue should they become a threat.

Also explain methods used to prevent the threats and respond to the threats when they occur.

Issue	Characteristics	Effects	Methods of Prevention	Methods of Response
<p><i>Cyber-bullying and stalking</i></p>	<p><i>'Bullying' is usually used to refer to children and 'stalking' refers to adults.</i></p> <p><i>In this context, it is the use of DCTs such as mobile phones or e-mail to harass someone, often to the point where they feel persecuted or in danger. This may be done by obsessive emailing or texting, sending offensive materials through email, defamation in public or workplace electronic forums, using online information to find out where someone lives and then following them etc.</i></p>	<p><i>A person may suffer serious stress, anxiety, loss of standing amongst colleagues and their employer. They may also feel physically threatened and have to relocate to try to escape the person.</i></p>	<p><i>Never give out personal information on social sites or in the public arena.</i></p> <p><i>Do not give out personal information over email.</i></p> <p><i>Do not send threatening emails or insult anyone over electronic means.</i></p> <p><i>Ensure your encryption on your phone and email is up to date and operational.</i></p> <p><i>If someone you know sends you a threatening or offensive email, tell them that you do not want them to do that and then block them.</i></p> <p><i>Use a good anti-spyware program.</i></p>	<p><i>Contact your manager and ISP.</i></p> <p><i>Keep hard and soft copies of all harassing emails, and save texts.</i></p> <p><i>Change your password, cellphone number and email address.</i></p>

Issue	Characteristics	Effects	Methods of Prevention	Methods of Response
Piracy	<i>This is breaching copyright for electronic and audiovisual works such as DVDs or music.</i>	<i>The artist or producer loses revenue as the work is not paid for by the viewer.</i>	<i>Copy protection on disks. Try to avoid placing the work on-line. Ensure a copyright warning is placed on the disk.</i>	<i>Criminal proceedings may be taken.</i>
Privacy	<i>A lot of personal information on clients and other sensitive information is held electronically, such as on databases. This can be illegally obtained through phishing, Trojan horse viruses and other methods.</i>	<i>The organisation may find themselves up before the Privacy Commissioner. Sensitive information such as new patents may be stolen by competitors. Personal information may be used for identity theft or by cyber-stalkers.</i>	<i>Password protection on all files containing personal or commercially sensitive information. Ensure mobile devices such as phones and laptops have a high level of encryption. Shred all confidential documents. Use a good anti-spyware program.</i>	<i>Legal action. The Privacy Commissioner may become involved.</i>
Copyright	<i>Reproducing work that someone else owns the copyright to, without their permission. With DCT this is now very easy to do, thanks to the existence of technology such as scanning. The work reproduced may be written, visual or audio.</i>	<i>As for piracy, this can lead to loss of revenue for the author as a fee should be paid.</i>	<i>Ensure that anything reproduced is not already held under copyright and any material your organisation wishes to protect is copyright.</i>	<i>Legal action may be required.</i>

Issue	Characteristics	Effects	Methods of Prevention	Methods of Response
Phishing	<p><i>This is using fraudulent means to electronically obtain sensitive information such as usernames, passwords and credit card numbers.</i></p> <p><i>For example emails may be received that impersonate an organisation that you know such as your bank asking you to verify your login details. If you respond the hyperlink looks like it sends you to the bank's site but it actually sends you to the phisher's webpage. They then have access to your personal details.</i></p>	<p><i>You can find yourself a victim of identity theft – the phisher may use your credit card details to purchase items or steal money from your bank account.</i></p>	<p><i>Never respond to such emails. Banks do not ask you to verify details in that way.</i></p> <p><i>If an organisation asks you to verify or give account details on line, phone them.</i></p> <p><i>Instead of using hyperlinks, type the organisation's address in the URL yourself if you know it.</i></p> <p><i>Look for security certificates and the browser's secure site icon such as a closed padlock.</i></p> <p><i>Change passwords frequently.</i></p>	<p><i>Tell the organisation such as the credit card company and the ISP.</i></p> <p><i>Cancel your credit card and change your bank account details, user name, password etc.</i></p>
Identify Theft	<p><i>This is someone illegally obtaining your personal details and impersonating you for financial gain or other benefits.</i></p>	<p><i>You may suffer financial loss or a bad credit rating. You may also find yourself liable for fines you didn't incur.</i></p>	<p><i>As for phishing.</i></p> <p><i>Check your credit report regularly to ensure no-one has tried to obtain credit in your name.</i></p> <p><i>Do not give out personal</i></p>	<p><i>Contact the organisation, your ISP and the police.</i></p> <p><i>Change your password and username.</i></p>

Issue	Characteristics	Effects	Methods of Prevention	Methods of Response
			<p><i>information.</i></p> <p><i>Ensure your system has very good encryption.</i></p> <p><i>Change passwords and usernames regularly. Use passwords that have a combination of letters and numbers and don't spell anything.</i></p> <p><i>Report the theft of documents such as passports and cancel stolen credit cards immediately.</i></p> <p><i>Use a good anti-spyware program.</i></p>	
Scams	<p><i>There are many email scams in operation such as 'You have won a lottery' when you never bought a ticket and 'Invest in our company in Nigeria'. They always ask you eventually for money and bank account details.</i></p>	<p><i>They keep any money you send and you never see a cent. Or they may use the details they have gained to fraudulently obtain further money from you.</i></p>	<p><i>If it seems to good to be true it more than likely is. Do not respond to these scams.</i></p> <p><i>If you are suspicious check with organisations such as Consumer Institute.</i></p>	<p><i>Don't! Report them to your ISP and the police.</i></p>

Issue	Characteristics	Effects	Methods of Prevention	Methods of Response
Viruses	<i>Viruses are normally malicious programs that attach themselves to files or emails and then spread through computer systems causing damage or, in the case of a Trojan Horse, stealing information such as recording keystrokes.</i>	<i>Files may become corrupted or the damage may be to the point that the hard drive erases itself. Information may be obtained to be used for identity theft.</i>	<i>Use a very good anti-virus program and firewall. Ensure that they are both up to date.</i>	
Spam	<i>This is sending email to a large amount of people that is unsolicited – the electronic version of junk mail.</i>	<i>Your email inbox can get clogged with unwanted messages, and your email address used by spammers to send spam to others.</i>	<i>Do not give your work or every day email address out to other organisations (unless they're work related) – have a different email for sites you sign up to such as forums. You can use the junk mail filter built in to most email and webmail programs. Do not respond to spam – they then know they have a valid email address and send you more.</i>	<i>Contact your IT manager or ISP. Unsolicited email is illegal in New Zealand.</i>

Assessment Task Two – Elements 2 and 3

Introduction

The purpose of this task is to assess the learner's ability to use and manage DCTs.

Instructions

The learner must be observed using and managing a minimum of three DCTs in their workplace. The observer can be yourself or someone approved by you such as the learner's team leader.

The learner must:

- Follow all current conventions for layout, etiquette and protocol relating to the DCTs.
- Ensure the content of the communication meets the current conventions for its purpose, target audience and the DCTs themselves.
- Manage the DCTs (eg save. delete etc)

The Observer Feedback Form details the requirements of the task. Please ensure it is completed during the observation. You may wish to discuss the learner's performance with them, especially if you are not the observer.

The evidence required for assessment task one will include:

- Completed checklist.
- Assessor's notes where relevant.

Assessment Guide

Use the table below to assess the learner’s competence for unit standard 25662. The Learning Assessment Guide for this unit also includes this Assessment Guide.

Element	Task	Evidence required	Judgement
<p>One</p> <p>Explain the use of digital communications technologies.</p>	<p>One</p>	<p>Learner provides answers to questions relating to:</p> <p>The types of DCTs used in terms of the technology used.</p> <p>Inappropriate situations for using DCTs.</p> <p>Ethical and legal issues associated with the use of DCTs and methods of preventing and responding to DCT threats.</p>	<p>Learner correctly explains the technology used for three DCTs. Technology may include hardware and or software.</p> <p>Learner explains situations where using DCTs would be inappropriate. Explanation must cover personal situations, business situations, time factors and cost factors and be in terms of the responsibilities of the user and current protocols.</p> <p>Learner explains at least two ethical and legal issues associated with the use of DCTs . They must also explain two ways of preventing each of the two issues becoming threats and give methods of response to the threats.</p> <p>Threats and ethical and legal issues include:</p> <ul style="list-style-type: none"> • cyber-bullying and stalking • privacy • copyright • piracy • identity theft • scams • viruses • spam • phishing.

Element	Task	Evidence required	Judgement
Two Use DCTs.	Two	Observation checklist completed confirming learner has used a minimum of three DCTs.	<p>Learner is observed for three DCTs:</p> <p>Producing communication that meets current conventions for the:</p> <ul style="list-style-type: none"> • Purpose of the communication. • Its target audience. • The DCT used. <p>Observing current conventions for:</p> <ul style="list-style-type: none"> • Layout • Etiquette • Protocols
Three Manage DCTs.	Three	Observation checklist completed confirming learner has managed a minimum of three DCTs.	<p>Learner is observed correctly managing a minimum of three DCTs. This may include but is not limited to:</p> <ul style="list-style-type: none"> • Prioritise • Delete • Save • Create and use folders • Filters and templates • Backup data • Automated message use • Add signatures and/or attachments.

Use digital communications technologies

25662 V1

Level 2

Credits 3

Purpose People credited with this unit standard are able to: explain the use of, use, and manage digital communications technologies.

Subfield Computing

Domain Generic Computing

Status Registered

Status date 22 May 2009

Date version published 22 May 2009

Planned review date 31 December 2013

Entry information Open.

Replacement information This unit standard replaced unit standard 5941.

Accreditation Evaluation of documentation by NZQA.

Standard setting body (SSB) NZQA National Qualifications Services

Accreditation and Moderation Action Plan (AMAP) reference 0226

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

Special notes

- 1 Definitions
Digital communications technologies (DCTs) refers to digital tools that enable interaction and communication. These may include but are not limited to – email, Short Message Service (SMS), Multimedia Message Service (MMS), Voice-over-Internet protocol (VoIP), social software, blog, wiki, forum, usenet, mailing lists, websites.
Recognised conventions for the purpose of this unit standard mean the generally accepted and/or documented practice of an organisation, workplace, or user group. Conventions may vary depending on the context of the communication, however some common examples are: use of capitals, abbreviations or acronyms; naming; use of hyperlinks; appropriateness of content; referencing of source material.
- 2 Legislation relevant to this unit standard includes but is not limited to the:
Copyright Act 1994,
Health and Safety in Employment Act 1992,
Privacy Act 1993,
Unsolicited Electronic Messages Act 2007,
and their subsequent amendments.

- 3 An assessment resource to support computing unit standards (levels 1 to 4) can be found on the NZQA website at <http://www.nzqa.govt.nz/providers/resources/index.html>.

Elements and performance criteria

Element 1

Explain the use of digital communications technologies (DCTs).

Performance criteria

- 1.1 Types of DCTs are explained in terms of the technology they use.
- Range may include but is not limited to – hardware or software technology. A minimum of three DCTs are explained.
- 1.2 Situations when DCTs are inappropriate are explained in terms of user responsibilities and protocols.
- Range includes but is not limited to – personal, business, time, cost.
- 1.3 Ethical and legal issues associated with the use of DCTs are explained in terms of their characteristics and effect.
- Range may include but is not limited to – cyber-bullying, stalking, privacy, copyright, piracy, identity theft, scams, viruses, spam. Evidence of two is required.
- 1.4 Methods of preventing and responding to DCT threats are explained in terms of their characteristics and effect.
- Range threats may include but are not limited to – cyber-bullying, phishing, stalking, privacy, copyright, piracy, identity theft, viruses, spam. Methods of preventing may include but are not limited to – use of protection software, regular virus scans. Methods of responding may include but are not limited to – non-response to communications, reporting to appropriate authority. Evidence is required for two threats and two methods of preventing.

Element 2

Use DCTs.

Range a minimum of three DCTs are used.

Performance criteria

- 2.1 The content of the digital communication meets recognised conventions for the purpose, target audience, and the DCT used.
- 2.2 The DCTs are used according to recognised conventions.
- Range may include but is not limited to – layout, etiquette, protocols.

Element 3

Manage DCTs.

Range a minimum of three DCTs are managed.

Performance criteria

3.1 DCTs management is demonstrated according to the controls of the technology used.

Range DCTs management may include but is not limited to – prioritise, delete, save; create and use folders, filters and templates; backup data; automated message use; add signatures and/or attachments.

Please note

Providers must be accredited by NZQA, or an inter-institutional body with delegated authority for quality assurance, before they can report credits from assessment against unit standards or deliver courses of study leading to that assessment.

Industry Training Organisations must be accredited by NZQA before they can register credits from assessment against unit standards.

Accredited providers and Industry Training Organisations assessing against unit standards must engage with the moderation system that applies to those standards.

Accreditation requirements and an outline of the moderation system that applies to this standard are outlined in the Accreditation and Moderation Action Plan (AMAP). The AMAP also includes useful information about special requirements for organisations wishing to develop education and training programmes, such as minimum qualifications for tutors and assessors, and special resource requirements.

Comments on this unit standard

Please contact the NZQA National Qualifications Services nqs@nzqa.govt.nz if you wish to suggest changes to the content of this unit standard.