SVQ for IT Users (ITQ) — level 3 (SCQF level 6)

F9A2 04: Using the Internet 3

5 SCQF credit points at SCQF level 6

Description: This is the ability to set up and use appropriate connection methods to access the internet; make the best use of browser software tools and techniques to search for, retrieve and exchange information using a browser or public search engine, and work safely and securely online.

Outcome **On completion of this Unit the candidate should be able to:**	**Skills and Techniques**	**Knowledge and Understanding**
1 Select and set up an appropriate connection to access the internet.	1 Select and **set up an internet connection** using an appropriate combination of hardware and software. 2 Recommend a connection method for internet access to meet identified needs. 3 Diagnose and solve Internet connection problems.	1 Identify different types of **connection methods** that can be used to access the internet. 2 Explain the **benefits and drawbacks** of different connection methods. 3 Analyse the issues affecting different groups of **users**.
2 Set up and use browser software to navigate web pages.	1 Select and use **browser tools** to navigate web pages effectively. 2 Adjust and monitor **browser settings** to maintain and improve performance. 3 Customise browser software to make it easier to use.	1 Explain when to change browser settings to aid navigation. 2 Explain when and how to improve **browser performance**.
3 Use browser tools to search effectively and efficiently for information from the internet.	1 Select and use appropriate **search techniques** to locate information efficiently. 2 Manage and use **references** to make it easier to find information another time. 3 **Download,** organise and store different types of information from the internet.	1 Evaluate how well **information meets requirement**s.

Outcome On completion of this Unit the candidate should be able to:		Skills and Techniques		Knowledge and Understanding	
4	Use browser software to communicate information online.	1 2	Select and use appropriate tools and techniques to **communicate information** online. **Share** and **submit information** online using appropriate language and moderate content from others.	2	Identify and analyse opportunities to create, post or publish material to websites.
5.	Develop and apply appropriate safety and security practices and procedures when working online.	1 2 3	Work responsibly and take appropriate **safety and security precautions** when working online. Keep information secure and manage **user access** to online sources securely. Develop and promote **laws, guidelines and procedure**s for safe and secure use of the internet.	1 2 3 4	Explain the **threats to system performance** when working online. Explain the **threats to information security** and integrity when working online. Explain the **threats to user safety** when working online. Explain how to **minimise internet security risks**.

Note: The **emboldened** items are exemplified in the Support Notes.

Evidence Requirements

Completion of a portfolio (manual, electronic or combination) to cover all of the Skills and Techniques and Knowledge and Understanding points stated above. The evidence generated should adhere to the Assessment Strategy for this award and encompass a range of evidence types.

General information

This Unit equates to NOS (National Occupational Standards for IT Users 2009) INT: Using the Internet level 3. It has a stated number of SCQF credit points = 5 at SCQF level 6.

Support Notes

Summary

A SCQF level 6 (ITQ level 3) user can advise on and set up an internet connection to meet a variety of user needs. They can also make efficient use of advanced internet software tools and techniques to search for and exchange information for complex and non-routine activities.

Internet tools and techniques will be defined as 'advanced' because:

- the software tools and functions required will be described as complex because at times they involve having the idea that there may be a tool or function to do something (eg improve efficiency or create an effect), exploring technical support, self-teaching and applying
- the range of techniques required for searching and exchanging information will be complex, and the selection process may involve research, identification and application

An activity will typically be 'complex and non-routine' because:

- the task is likely to require research, identification and application
- the context is likely to require research, analysis and interpretation; and
- the user will take full responsibility for searching for and exchanging the information

Examples of context which illustrate typical activities which might be undertaken by users:

- setting up an Internet connection for use by others
- developing and promoting organisational guidelines and procedures for Internet safety
- setting up and moderating the content of a discussion forum

Examples of content are given separately for highlighted text, where explanatory notes are required on terminology in the Outcomes, and do not form part of the standards. Such examples are not meant to form a prescriptive list for the purposes of assessment but rather to amplify and interpret the generic terms used in the performance criteria in the light of current usage of ICT systems and software. These examples are subject to change as new tools and techniques become commonplace and older ones drift out of use.

The examples given below are indicative of the learning content and are not intended to form a prescriptive list for the purpose of assessment.

Outcome 1

Connection methods: LAN, VPN, modem, router, wireless, broadband, dial-up, cable, DSL; mobile phone with wireless application protocol (WAP) or 3rd Generation (3G) technology; intranet server (eg via parallel, serial or USB connections); *extranet*.

Benefits and drawbacks of connection methods: Speed, stability, accessibility, *frequency of connection problems, additional services offered by ISP*, *cost, security.*

Users: New users, learners, those with restricted access, those with disabilities.

Set up an internet connection: Identifying and selecting ISP, connecting hardware, installing and configuring software, setting up and testing operation of connection; limiting access.

Outcome 2

Browser tools: Enter, back, forward, refresh, history, bookmark, new window, new tab, Toolbar, search bar, address bar; home, go to, follow link, URL; save web address, *save as, downloads, temporary files.*

Browser settings: Security, pop-ups, appearance, privacy, personalisation, accessibility, software updates, temporary file storage, *browser options, add-ons, RSS feeds, connections, search settings, content*.

Browser performance: Delete cache, delete temporary files, work offline, save websites, *benchmark tests.*

Outcome 3

Search techniques: Search key words, quotation marks, search within results, relational operators, 'find' or search tools; *search engine features*, multiple search criteria, *Boolean operators*, wild cards.

Information requirements: Reliability, accuracy, currency, sufficiency, relevance, level of detail; Recognise intention and authority of provider, bias; *synthesise information from a variety of sources; verify information.*

References: History, favourites, manage bookmarks and links, RSS, data feeds, saved search results.

Download information: Webpage, website; images, text, numbers, sound, games, video, TV, music; *software, patches.*

Outcome 4

Communicate information: Saved information (pod-casts, text, images), real time information (blogs, instant messaging; *virtual meetings*), file transfer protocol [FTP], hypertext transmission protocol [http], VOIP.

Share information sources: Send link, send webpage reference lists, *data feeds.*

Submit information: Fill-in and submit web forms; ratings, reviews, recommendations; wikis; discussion forums; interactive sites; netiquette.

Outcome 5

Threats to system performance: Unwanted e-mail (often referred to as 'spam'), malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers) and hackers; hoaxes.

Safety precautions: Firewall settings, Internet security settings; report inappropriate behaviour; report security threats or breaches; netiquette, content filtering, avoid inappropriate disclosure of information, carry out security checks, proxy servers.

Information security: Username and password/PIN selection and management, password strength, online identity/profile; real name, pseudonym, avatar; what personal information to include, who can see the information, withhold personal information.

Threats to information security: Malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers), hackers, phishing and identity theft.

Threats to user safety: Abusive behaviour ('cyber bullying'), inappropriate behaviour and grooming; abuse of young people; false identities; financial deception, identity theft.

Minimise risk: Virus-checking software, anti-spam software, firewall; treat messages, files, software and attachments from unknown sources with caution, internet settings, block sites, parental controls.

Laws, guidelines and procedures: Set by employer or organisation relating to Health and safety, security; equal opportunities, disability; Laws: relating to copyright, software download and licensing, digital rights*, IPR, health and safety.*

Guidance on examples of evidence

Typical examples of evidence for Outcome 1

Assessor checklist which records candidate competence in setting up a connection to the Internet – hardware and software. Extended response questions which test knowledge of connection types, their benefits and drawbacks and user group issues.

Typical examples of evidence for Outcome 2

Assessor checklist which records candidate competence in customising and using browser software for effective web searches. Extended response questions which test candidate competence in changing, and when to change, browser settings. Candidate product evidence – web pages saved electronically or printed.

Typical examples of evidence for Outcome 3

Assessor checklist which records successful candidate information location using an appropriate search strategy. Candidate product evidence to demonstrate that information found meets user requirements. Candidate evaluation on how well, found information, is fit for purpose.

Typical examples of evidence for Outcome 4

Assessor checklist which demonstrates candidate competence in communicating on line — downloading, uploading and submitting (use of forms etc). Candidate product evidence supporting communication activities — hard copy or electronic.

Typical examples of evidence for Outcome 5

Assessor checklist which records candidate competence in the development and application of appropriate online safety and security processes. Candidate statement or extended response question which demonstrate candidate competence in explaining threats to system performance, information security, user safety, minimisation of such risks and appropriate and relevant legislation covering on line activities and behaviour.

Disabled candidates and/or those with additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering whether any reasonable adjustments may be required. Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**