National Unit specification: general information

Unit title: Internet Safety (SCQF Level 4)

Unit code: H1F6 10

Superclass: CB

Publication date: May 2012

Source: Scottish Qualifications Authority

Version: 02

Summary

This Unit is about the knowledge and skills required to work safely and responsibly online, in the context of activities that are routine and familiar. On completion of this Unit, the candidate will understand the risks of working online and be able to take appropriate precautions to safeguard themselves and others and protect data and computer systems. The contents of this Unit include dealing with unwanted communications, protecting against identity theft, protecting systems against viruses, and other threats. This free-standing Unit is suitable for a wide range of candidates and is particularly appropriate for young people, parents and mature Internet users.

Outcomes

1 Describe the risks that exist when using the Internet.
2 Safeguard self and others when working online.
3 Take precautions to maintain data security and system performance.
4 Adhere to the legal constraints, guidelines and procedures that apply when working online.

Recommended entry

Entry is at the discretion of the centre. No previous knowledge or experience of computers or the Internet is required. However, it would be advantageous if candidates possessed basic IT skills which could be evidenced by having achieved Unit DO1D 10 *Information Technology (*SCQF level 4*)* and previous experience of using the Internet.

National Unit specification: general information (cont)

Unit title: Internet Safety (SCQF Level 4)

Credit points and level

1 National Unit credit at SCQF level 4: (6 SCQF credit points at SCQF level 4*)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

Core Skills

Achievement of this Unit gives automatic certification of the following Core Skills component:

Complete Core Skill	None
Core Skill component	Critical Thinking at SCQF level 4

There are also opportunities to develop aspects of Core Skills which are highlighted in the Support Notes of this Unit specification.

National Unit specification: statement of standards

Unit title: Internet Safety (SCQF Level 4)

Acceptable performance in this Unit will be the satisfactory achievement of the standards set out in this part of the Unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Outcome 1

Describe the risks that exist when using the Internet.

Performance Criteria

(a) Identify risks to user safety and privacy.
(b) Identify risks to data security.
(c) Identify risks to system performance and integrity.
(d) Describe how to minimise Internet risks.
(e) Describe factors that affect the reliability of information on websites.

Outcome 2

Safeguard self and others when working online.

Performance Criteria

(a) Take precautions to ensure own safety and privacy.
(b) Protect personal information online.
(c) Carry out checks on others' online identity.
(d) Describe the forms and features of cyberbullying.
(e) Explain when and how to report online safety issues.
(f) Identify where to get online help and information on e-safety.

Outcome 3

Take precautions to maintain data security and system performance.

Performance Criteria

(a) Take appropriate precautions to maintain data security.
(b) Take appropriate precautions to maintain system performance and integrity.
(c) Use appropriate browser safety and security settings to protect self and system.
(d) Use appropriate software safety and security settings to protect self.

National Unit specification: statement of standards (cont)

Unit title: Internet Safety (SCQF Level 4)

Outcome 4

Adhere to the legal constraints, guidelines and procedures that apply when working online.

Performance Criteria

(a) State the legal constraints on the uploading and downloading of software and other digital content.
(b) State the legal constraints on online behaviour.
(c) Adhere to guidelines and procedures for the safe use of the Internet.

Evidence Requirements for this Unit

Evidence is required to demonstrate that candidates meet the requirements of all the Outcomes and Performance Criteria. This will be in the form of written and/or oral responses to questions for the knowledge elements, and performance evidence for the skills elements. Most Outcomes contain both practical and theoretical aspects. This is exemplified in the Assessment Support Pack for the Unit which can be obtained from SQA.

The assessment of knowledge and understanding will be combined into a single written or oral assessment that samples the candidate's knowledge to the standards specified in the Performance Criteria. This assessment should be timed, done under controlled conditions, and without access to reference material (closed-book). The candidate's performance in this assessment must satisfy the assessor that s/he has gained the requisite knowledge and possesses a sufficient understanding of the key concepts in this Unit.

The assessment of skills will require the candidate to maintain a record of his/her activities during this Unit. The record may be written or oral or visual or a combination of these. The record should be maintained over the life of the Unit, and record the key activities carried out by the candidate during this period. The completed record of activities should state the specific activities carried out by the candidate, and provide contextual information to satisfy the assessor that the candidate has carried out the activity to the standards specified in the associated performance criterion/criteria. This record can be completed at a time and location convenient to the candidate. However, it must be maintained on a regular basis, and must be written in the first person, using the candidate's own words. The completed record must be authenticated by the assessor, who must confirm that the record is an accurate log of the candidate's activity over the duration of the Unit.

National Unit specification: support notes

Unit title: Internet Safety (SCQF Level 4)

This part of the Unit specification is offered as guidance. The support notes are not mandatory.

While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this Unit

The overall aim of this Unit is to enable candidates to work safely and responsibly online. The Unit will provide candidates with information about the safety factors and legal considerations which need to be taken account of when using the Internet and give them practical experience of using these. It is anticipated that the Unit will be delivered over an extended period of time, during which the candidate can be observed in their natural environment applying his/her knowledge of Internet safety. The Unit covers all of the skills outlined in the 'Internet Safety for IT Users' qualification produced by e-Skills, the Sector Skills Council for Business and IT.

The current context for this Unit is one of concern about the safety of young people on the Internet. This environment is partly the result of media stories relating to (for example) the abuse of young people or the financial deception of more mature users. An important Outcome of this Unit is to re-assure users that the Internet is a relatively safe environment so long as the appropriate precautions are followed. The broad context of this Unit is one of encouraging the safe and responsible use of the Internet — not discouraging its use through negative stories or obtrusive safety precautions. The Internet should be presented as a unique human achievement with huge potential for education and communication — but with potentially serious consequences if not used correctly. Particular attention should be paid to the risks involved in accessing the Internet from mobile devices.

Support materials are available for this Unit including online teaching, learning and assessment resources. Please contact SQA for additional information. The precise contents of this Unit will change over time, as Internet threats come and go and legislation is introduced or repealed. The following guidance exemplifies the Standards in terms of contemporary technologies, threats and legislation.

Outcome 1

This Outcome relates to the risks that can exist when using the Internet.

Performance criterion (a) relates to identifying risks to user to safety and privacy. Candidates should be aware that threats to user safety include abusive behaviour ('cyberbullying'), inappropriate behaviour and grooming. They should be aware that these threats can appear in a variety of different contexts, eg text messages, chat rooms, e-mail, social networking sites and instant messaging. They should also be aware of the need to minimise their 'digital footprint' by minimising the amount of personal information they reveal online.

Performance criterion (b) relates to identifying risks to data security. Candidates should be aware that risks to data security include malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers), hackers, phishing and identity theft and should be able to identify examples from all of these categories.

Performance criterion (c) relates to identifying risks to system performance and integrity.

Candidates should be aware that threats to system performance and integrity include unwanted e-mail (often referred to as 'spam'), malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers) and hackers, and should be able to identify examples of all of these categories. Candidates should also be made aware of non-existent ('hoax') threats (such as virus hoaxes) and emerging threats (which include 'ransomware').

Performance criterion (d) relates to minimising internet risks. Candidates should be aware of the steps they can take to minimise internet risks, including withholding personal information, reporting incidents to a responsible adult and making correct use of browser and social network security settings.

Performance criterion (e) relates to the factors that affect the reliability of information on websites. Candidates should be aware the information found online cannot always be assumed to be reliable and should know how to check factors such as scope of coverage, authority, objectivity, accuracy and timeliness.

Outcome 2

This Outcome relates to safeguarding self and others when working online.

Performance criterion (a) relates to taking appropriate precautions to ensure own safety and privacy. Candidates should be aware that precautions for maintaining user safety include content filtering, proxy servers, monitoring and reporting user behaviour and withholding personal information. The need to select non-trivial usernames and passwords should also be taught. Detailed advice should be provided on password selection, including the importance of selecting passwords of differing strengths to reflect their varying applications.

Performance criterion (b) relates to protecting personal information online, Candidates should be aware of the need to restrict the amount of personal information they reveal online.

Performance criterion (c) relates to carrying out checks on others' online identity. Candidates should be aware that people they encounter online may not be what they appear to be and should take steps to confirm their identity, eg: by checking with others who may know them. They should also be aware of the use of WHOIS to check the ownership of domain names.

Performance criterion (d) relates to describing the forms and features of cyberbullying. Candidates should be aware that cyberbullying is unacceptable and should be reported to the relevant authorities. They should know that cyberbullying can take many forms, eg: text messaging, e-mail, instant messaging, comments on social networking sites, videos, etc.

Performance criterion (e) relates to identifying when and how to report online safety issues. Candidates should know what types of issues require to be reported and how to report them, particularly using the Click CEOP button and the CEOP website (http://ceop.police.uk/).

Performance criterion (f) relates to identifying where to get online help and information on e-safety. Candidates should be aware of sources of online help and information, including http://www.thinkuknow.co.uk/ and http://www.childline.org.uk.

National Unit specification: support notes (cont)

Unit title: Internet Safety (SCQF Level 4)

Outcome 3

This Outcome relates to taking precautions to maintain data security and system performance.

Performance criterion (a) relates to taking appropriate precautions to maintain data security. Candidates should be aware that precautions for maintaining data security include firewalls, software for detecting and disabling malicious programs or malware (including viruses, worms, trojans, spyware, adware and rogue diallers) and e-mail filtering software (spam filters). They should be able to describe the precautions which can be taken in all these categories, including the use of Internet security suite, which may cover more than one category of threat. If an Internet security suite is not used, a range of different software programs will have to be collected to provide the cover for each of the various threats. They should also be aware that while system performance and data security are separate topics, the precautions taken may end up addressing the same issues.

Performance criterion (b) relates to taking appropriate precautions to maintain system performance and integrity. Candidates must be aware that precautions for maintaining system performance and integrity include firewalls, software for detecting and disabling malicious programs or malware (including viruses, worms, trojans, spyware, adware and rogue diallers) and e-mail filtering software (spam filters). They must be able to describe the precautions which can be taken in all these categories, including the use of Internet security suites, which may cover more than one category of threat. If an Internet security product is not used, a range of different software programs will have to be collected to provide the cover for each of the various threats.

Performance criterion (c) relates to using appropriate browser safety and security settings. Candidates should be aware of the need to select the correct level of browser safety and security settings and know how to do this for major browsers such as Internet Explorer and Firefox.

Performance criterion (d) relates to using appropriate client software safety and security settings. Candidates should be aware that many sites, including major social networking sites, allow users to configure safety and security settings, but the default settings are not always the best option.

Outcome 4

This Outcome is about adhering to the legal constraints, guidelines and procedures which apply when working online.

Performance criterion (a) relates to stating legal constraints on the uploading and downloading of software and other digital content. Candidates should be aware that legal constraints on the uploading and downloading of software and data, including music and videos, include copyright and digital rights management, such as restricting the number of times a media file can be copied or converted to another format. Software licensing should be considered (such as freeware and shareware).

National Unit specification: support notes (cont)

Unit title: Internet Safety (SCQF Level 4)

Performance criterion (b) relates to stating legal constraints on online behaviour. Candidates should be aware that legal constraints on online behaviour include protection of children legislation which prohibits grooming and inappropriate behaviour towards minors. Candidates should be introduced to 'netiquette' which describes the recommended conduct of users in various online environments. Libellous behaviour should also be discussed.

Performance criterion (c) is about adhering to guidelines and procedures for the safe use of the Internet. It is not sufficient for candidates to simply demonstrate knowledge of guidelines and procedures — they must be seen to apply these.

Guidance on learning and teaching approaches for this Unit

A practical hands-on approach to learning should be adopted to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before candidates commence these activities.

It is recommended that students gain hands-on experience of at least one example of each type of software mentioned in these Notes. While teaching will necessarily focus on a specific product, the generic features of the class of software should be emphasised.

An important Outcome for this Unit is that candidates develop an appropriate technical vocabulary. Terminology and underpinning knowledge should be introduced in a practical context.

The actual distribution of time between Outcomes is at the discretion of the centre. However, one possible approach is to distribute the available time equally over the four Outcomes, ie 10 hours per Outcome.

Throughout this Unit, candidate activities should relate to their personal or vocational interests. For example candidates should visit websites and chat rooms, and download content relating to their academic work, hobbies and pastimes, recreational and entertainment preferences or other topics that can genuinely hope to stimulate their interest. Teaching should be exemplified in terms of services and technologies that the candidate can relate to and are likely to use, such as community sites for older teenagers or online travel sites for more mature students.

The use of case studies is recommended.

This Unit may be delivered stand-alone or in conjunction with other Units. Where it is delivered alongside other Units, there is an opportunity to contextualise this Unit in terms of the contents of the other Unit(s) since this Unit's contents are generic and may be contextualised in a variety of ways.

National Unit specification: support notes (cont)

Unit title: Internet Safety (SCQF Level 4)

Guidance on approaches to assessment for this Unit

An integrative approach has been taken with all Outcomes being assessed through two instruments of assessment. All Outcomes contain both theoretical and practical content.

The assessment for the theoretical content may be in the form of an objective test consisting of a suitable number and range of questions to cover all Outcomes and Performance Criteria. It is anticipated that this assessment will be carried out towards the end of the Unit once candidates have had an opportunity to acquire the essential knowledge and understanding required to give them a realistic prospect to pass the assessment.

The assessment for the practical content consists of observing the candidate over an extended period of time during which the candidate is required to maintain a log of activity. It is recommended that this assessment is started at the earliest opportunity, as soon as the candidate has acquired the necessary knowledge and skills to permit him/her to commence appropriate tasks.

The assessment for this Unit is well-suited to online assessment. The assessment of knowledge and understanding may be assessed using an item bank of appropriate questions; and the assessment of practical abilities may be assessed using a digital repository for the candidate's log, such as an e-portfolio or web log.

The assessment of knowledge and understanding will be combined into a short test lasting no more than 50 minutes. These should be answered in a single sitting under controlled conditions in closed-book environment under supervision.

The performance evidence will consist of a log of the candidate's activity. The log will provide a record of candidate activity during this Unit, which will provide evidence that the candidate has satisfied the relevant Performance Criteria. It will consist of a first person log of candidate activity over an extended period of time (including what the candidate has learned while undertaking this Unit). The log will provide evidence that the candidate has behaved appropriately, carried out suitable security checks, worked securely and reported inappropriate behaviour (if any) and security threats or breaches (if any). Candidate activity must satisfy the prescribed Performance Criteria, and must therefore embrace a sufficient range of activities to permit the candidate to satisfy these criteria. The log may be completed at a time and location to suit the candidate; it is anticipated that some activity may take place outside of the formal learning environment. The log must be authenticated by the assessor (or approved mentor) who must confirm that the log is an accurate record of candidate activity.

This Unit may be delivered in a distance learning/online mode. In these circumstances centres must take appropriate steps to authenticate the candidate's evidence. This can be done in a variety of ways such as the use of webcams or VOIP.

A delivery guide for centres that wish to deliver this Unit via the Internet is available from SQA.

National Unit specification: support notes (cont)

Unit title: Internet Safety (SCQF Level 4)

Opportunities for the use of e-assessment

E-assessment may be appropriate for some assessments in this Unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all candidate evidence and that conditions of assessment as specified in the Evidence Requirements are met, regardless of the mode of gathering evidence. Further advice is available in *SQA Guidelines on Online Assessment for Further Education (AA1641, March 2003), SQA Guidelines on e-assessment for Schools (BD2625, June 2005)*.

Opportunities for developing Core Skills

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when candidates achieve the Unit, their Core Skills profile will also be updated to show they have achieved Critical Thinking at SCQF level 4.

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**

History of changes to Unit

Version	Description of change	Date
02	Core Skills Component Critical Thinking at SCQF level 4 embedded.	17/05/2012