



National Unit Specification: general information

UNIT Internet Safety (Intermediate 1)

CODE F0H5 10

COURSE

SUMMARY

The Unit is designed to enable candidates to make safe and legal use of the Internet. The Unit will provide candidates with information about the safety factors and legal considerations which need to be taken into account when using the Internet, and give candidates practical experience in taking safety precautions and operating within legal constraints. The contents of this Unit include dealing with unwanted e-mail, protecting against identity theft, and 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 Identify threats that can exist when using the Internet.
- 2 Describe safety precautions which should be taken when using the Internet.
- 3 Describe legal constraints which apply when using the Internet.
- 4 Take appropriate safety precautions and operate within relevant legal constraints when using the Internet.

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.

Administrative Information

Superclass: CD

Publication date: August 2006

Source: Scottish Qualifications Authority

Version: 01

© Scottish Qualifications Authority 2006

This publication may be reproduced in whole or in part for educational purposes provided that no profit is derived from reproduction and that, if reproduced in part, the source is acknowledged.

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. The cost for each Unit specification is £2.50. (A handling charge of £1.95 will apply to all orders for priced items.)

National Unit Specification: general information (cont)

UNIT Internet Safety (Intermediate 1)

CREDIT VALUE

1 credit at Intermediate 1 (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

There is no automatic certification of Core Skills or Core Skills components in the Unit.

National Unit Specification: statement of standards

UNIT Internet Safety (Intermediate 1)

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 the Scottish Qualifications Authority.

OUTCOME 1

Identify threats that can exist when using the Internet

Performance Criteria

- (a) Threats to system performance and system integrity are correctly identified.
- (b) Threats to data security are correctly identified.
- (c) Threats to user safety are correctly identified.

OUTCOME 2

Describe safety precautions which should be taken when using the Internet

Performance Criteria

- (a) Precautions for maintaining system performance and system integrity are accurately described.
- (b) Precautions for maintaining data security are accurately described.
- (c) Precautions for maintaining user safety are accurately described.

OUTCOME 3

Describe legal constraints which apply when using the Internet

Performance Criteria

- (a) Legal constraints on the downloading of software and data are accurately described.
- (b) Legal constraints on the use of online content are accurately described.
- (c) Legal constraints on construction of websites are accurately described.
- (d) Legal constraints on online behaviour are accurately described.

OUTCOME 4

Take appropriate safety precautions and operate within relevant legal constraints when using the Internet

Performance Criteria

- (a) System performance and system integrity are effectively maintained.
- (b) Data security is effectively maintained.
- (c) User safety is effectively maintained.
- (d) Copyright is correctly observed.

National Unit Specification: statement of standards (cont)

UNIT Internet Safety (Intermediate 1)

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 Outcomes 1 – 3 and performance evidence for Outcome 4.

The assessment of knowledge and understanding will be combined into a short test relating to Outcomes 1, 2 and 3, 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 for Outcome 4 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 performance criteria for Outcome 4. 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.

National Unit Specification: support notes

UNIT Internet Safety (Intermediate 1)

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 make safe and legal use of the Internet. 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.

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.

This Unit should ideally be delivered over an extended period of time to give candidates the opportunity to make safe and legal use of the Internet over an extended timeframe.

A wide range of support materials are available for this Unit including online teaching and learning resources. Please refer to the following website for further information: <http://www.netsafe.org.uk>.

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 identifying threats that can exist when using the Internet.

Performance criterion (a) relates to correctly identifying threats 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 (b) relates to correctly identifying threats to data security. Candidates should be aware that threats 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.

National Unit Specification: support notes (cont)

UNIT Internet Safety (Intermediate 1)

Performance criterion (c) relates to correctly identifying threats to user safety. 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 chat rooms, e-mail and instant messaging.

There is an opportunity in this Outcome to explore bias and the authenticity of information (using the URL to check the source of the information). While the formal evaluation of information is beyond the scope of this Outcome, basic information literacy should be explored.

Outcome 2

This Outcome relates to describing safety precautions which should be taken when using the Internet.

Performance criterion (a) relates to describing precautions for maintaining 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 (b) relates to describing precautions for maintaining 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 (c) relates to describing precautions for maintaining user safety. 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.

Outcome 3

This Outcome relates to describing legal constraints which apply when using the Internet.

Performance criterion (a) relates to legal constraints on the downloading of software and data. Candidates should be aware that legal constraints on the downloading of software and data 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 Internet Safety (Intermediate 1)

Performance criterion (b) relates to legal constraints on the use of online content. Candidates should be aware that legal constraints on the use of online content, such as text and graphics from web pages, include copyright, data protection and intellectual property rights.

Performance criterion (c) relates to legal constraints on the construction of websites. Candidates should be aware that legal constraints on the construction of websites include disability discrimination legislation, which specifies that websites must be made accessible to those with disabilities, and legislation relating to illegal content such as terrorist, pornographic and racist material.

Performance criterion (d) relates to 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.

Outcome 4

This outcome relates to candidates’ performance in taking appropriate safety precautions and operating within the relevant legal constraints when using the Internet.

It is anticipated that this Outcome will be carried out over an extended period of time, during which the candidate can be observed in their natural environment applying his/her knowledge of Internet safety.

Performance criterion (a) relates to precautions for maintaining system performance and integrity. Candidates should be aware that precautions for maintaining system performance and integrity include firewalls (which protect systems against intrusion), Internet security software (which protects against a range of threats including viruses, worms, trojans, spyware, adware and rogue diallers) and spam filters (which reject unwanted e-mail).

Performance criterion (b) relates to precautions for maintaining data security. Candidates should be aware that precautions for maintaining data security include firewalls (which protect systems against intrusion), Internet security software (which protects against a range of threats including viruses, worms, trojans, spyware, adware and rogue diallers) and spam filters (which reject unwanted e-mail).

Performance criterion (c) relates to precautions for maintaining user safety. Candidates should be aware that precautions for maintaining user safety include content filtering, proxy servers, monitoring and reporting user behaviour and withholding personal information.

Performance criterion (d) relates to downloading content in line with copyright restrictions. Candidates should be aware that copyright restrictions must always be taken into consideration when downloading content.

National Unit Specification: support notes (cont)

UNIT Internet Safety (Intermediate 1)

GUIDANCE ON LEARNING AND TEACHING APPROACHES FOR THIS UNIT

Although three of the four outcomes are theoretical in nature, 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 distribution of time is:

Outcome 1	7 hours
Outcome 2	7 hours
Outcome 3	6 hours
Outcome 4	20 hours

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 candidates 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.

GUIDANCE ON APPROACHES TO ASSESSMENT FOR THIS UNIT

An integrative approach has been taken with the four outcomes being assessed through two instruments of assessment. The first assessment covers Outcomes 1, 2 and 3, and the second assessment relates to Outcome 4.

The assessment for Outcomes 1, 2 and 3 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.

National Unit Specification: support notes (cont)

UNIT Internet Safety (Intermediate 1)

The assessment for Outcome 4 is a practical assessment consisting of observation of 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 (Outcomes 1-3) may be assessed using an item bank of appropriate questions; and the assessment of practical abilities (Outcome 4) may be assessed using a digital repository for the candidate's log (such as an e-portfolio or web log).

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.

CANDIDATES WITH DISABILITIES AND/OR ADDITIONAL SUPPORT NEEDS

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments or considering alternative Outcomes for Units. For information on these, please refer to the SQA document *Guidance on Alternative Assessment Arrangements for Candidates with Disabilities and/or Additional Support Needs*, which is available on SQA's website: www.sqa.org.uk.