National Unit Specification: general information

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

CODE F1FF 12

SUMMARY

This Unit is a mandatory Unit of PC Passport: Advanced but can also be undertaken as a free-standing Unit.

This Unit is designed to introduce candidates to complex issues relating to the internet and online communications. Candidates will develop knowledge of communications technology and different connection types and suitability of use. Candidates will also research and develop knowledge of security threats related to the internet and discover strategies to overcome these threats. Candidates will also publish information using a method of online communication.

This Unit is suitable for anyone that wishes to develop skills and understanding in the complex use of internet and online communications.

OUTCOMES

1 Identify complex issues for secure online communications.
2 Confirm secure communication settings and use these to send and receive encrypted e-mail.
3 Publish research findings on complex internet security risks and prevention strategies in an online communications format.

RECOMMENDED ENTRY

While entry is at the discretion of the centre, candidates would normally be expected to have attained one of the following, or equivalent:

- PC Passport: Internet and Online Communications (SCQF level 5)
- D973 11 Computer Networks (SCQF level 5)
- DM4F 11 The Internet (SCQF level 5)

Administrative Information

Superclass: CB

Publication date: August 2010

Source: Scottish Qualifications Authority

Version: 02

Additional copies of this Unit Specification can be purchased from the Scottish Qualifications Authority. Please contact the Customer Contact Centre, telephone 0845 279 1000.

National Unit Specification: general information (cont)

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

CREDIT VALUE

1 credit at Higher (6 SCQF credit points at SCQF level 6*)

**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 in this Unit.

The Unit provides opportunities for candidates to develop aspects of the following Core Skills:

- Information Technology (SCQF level 6)
- Communication (SCQF level 6)
- Problem Solving (SCQF level 6)

These opportunities are highlighted in the Support Notes of this Unit Specification.

National Unit Specification: statement of standards

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

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

Identify complex issues for secure online communications.

Performance Criteria

(a) Identify the Transmission Control Protocol/Internet Protocol (TCP/IP) communications model with reference to the role of devices and protocols.
(b) Identify internet addressing schemes.
(c) Identify different connection types and characteristics.
(d) Identify techniques used to ensure secure online communication.

OUTCOME 2

Confirm secure communication settings and use these to send and receive encrypted e-mail.

Performance Criteria

(a) Confirm level of system security settings.
(b) Send e-mail effectively using appropriate encryption methods.
(c) Receive and open encrypted e-mail messages.

OUTCOME 3

Publish research findings on complex internet security risks and prevention strategies in an online communications format.

Performance Criteria

(a) Conduct research into an agreed topic on internet security risk.
(b) Determine an appropriate prevention strategy to reduce risks of the agreed topic.
(c) Confirm the relevance and accuracy of research information.
(d) Create coherent content outlining the internet security risk and prevention strategy which is appropriately structured for the type of media.
(e) Publish the content in an appropriate online communications format.

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

EVIDENCE REQUIREMENTS FOR THIS UNIT

Evidence is required that candidates have achieved all Outcomes and Performance Criteria.

Candidates are encouraged to use the internet in any research, etc however the evidence produced must be the candidate's own words. Assessors should assure themselves of the authenticity of candidate's evidence.

Written and/or oral recorded, performance and product evidence is required which demonstrates that the candidate has achieved the requirements of all of the Outcomes and Performance Criteria.

Written and/or oral recorded evidence is required which demonstrates that the candidate has achieved Outcome 1 to the standard specified in the Outcome and Performance Criteria. The evidence for this Outcome should be obtained under controlled, supervised conditions. The assessment will be closed-book and should last no more than 45 minutes.

The instrument of assessment will provide opportunities for the Outcome to be fulfilled by means of sampling across the range of the content of Outcome 1. Where re-assessment is required, it should contain a different sample across the range of content of the Outcome. Achievement could be decided using a cut-off score. Each sample must include the following:

- Two layers of the TCP/IP model including the role of the layer, devices used and at least one TCP/IP protocol.
- Four characteristics of Internet Protocol (IP) addressing from: IP versions 4 and 6, version 4 classes, public and private IP addresses, subnet mask, gateway, Domain Name Service (DNS) and Network Address Translation (NAT).
- Two characteristics of different types of connection (wired and wireless) from: typical speeds, security and suitability of use, etc.
- Four different types of online security from within the following:
    - Current encryption algorithms
    - Digital signatures and certificates
    - Secure sockets
    - Proxy servers
    - Firewalls

For Outcome 2, performance evidence supplemented by an assessor observation checklist is required which demonstrates that the candidates can:

- Confirm level of internet security settings.
- Receive one encrypted e-mail and respond by sending an encrypted e-mail.

This evidence will be gathered under supervised open-book conditions. The evidence may be produced over an extended period of time.

National Unit Specification: statement of standards (cont)

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

For Outcome 3, product evidence in the form of published content is required to demonstrate that the candidate has achieved Outcome 3 to the standard specified in the Outcomes and Performance Criteria. This evidence will be gathered under supervised open-book conditions. The evidence may be produced over an extended period of time.

The published content must include:

- Research on a complex internet security risk and possible prevention strategies to minimise risks. The topic selected must be agreed by the candidate and assessor in advance of the research being carried out.
- Sufficient, relevant and accurate information with appropriate reference to information sources.
- Complex features of an application to produce information for online communication.
- Content related to one security risk, the nature of the risk, warning signs of a risk, what damage can be caused by the risk and how to protect against the risk. The content must be coherent and appropriately structured for the type of media used.

The Assessment Support Pack (ASP) for this Unit provides sample assessment materials including assessor checklists, practical tasks and an instrument of assessment for the knowledge and understanding of Outcome 1. Centres wishing to develop their own assessments should refer to the Assessment Support Pack to ensure a comparable standard.

National Unit Specification: support notes

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

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

This Unit may be delivered as a stand-alone Unit or in combination with other Units as part of a group of Units making up an award, eg PC Passport: Advanced.

This Unit is not designed as an introductory Unit. Candidates are expected to have good IT skills and are also expected to possess a basic knowledge of the factors affecting the performance of an internet connection.

The term *internet* is used to represent the full range of internet services which includes the world wide web, e-mail, file transfer, newsgroups and chat etc. This Unit can also be delivered using an intranet within a centre where there is limited availability of internet connections. The assessor must ensure that the intranet content and facilities are sufficient to satisfy the Outcomes and Performance Criteria.

This Unit does not map to the National Occupational Standards (NOS) for IT users as specified by the Sector Skills Council (E-Skills UK) and does not contain any Unit coverage of Areas of Competence.

Outcome 1

This Outcome relates to complex issues of internet and online communications. Candidates are introduced to an open system communications model. TCP/IP is a commonly used model and candidates should fully understand what happens to a communication at each of the layers and the protocols involved. Communication devices and characteristics should also be explained. Although troubleshooting is not assessed in this Unit candidates should be made aware of how the layered approach can be used to assist problem solving.

Candidates must understand the importance of internet addressing and should become familiar with IP addressing. This will include familiarity with the network connections to a system. Candidates should be able to recognise IP address schemes and classes where appropriate. The use of private and public addresses should be covered and candidates should know that Network Address Translation (NAT) allows the use of a private address to access the internet. The mapping of domain names to IP addresses should be covered. It is not necessary to include address resolution to MAC addresses.

Candidates should be introduced to both wired and wireless connections. The devices used in both types of connections should be covered as should the characteristics of both connections. Speed, range and reliability should be covered as a minimum. When covering wireless it is an ideal opportunity to introduce security issues.

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

Candidates should be aware of the need to use security methods such as encryption and keys. They should also be able to describe how these work to provide required security although it is not necessary to provide details of algorithms. Algorithms may include the following; Pretty Good Privacy (PGP), RSA, Data Encryption Standards (DES), versions, characteristics and strengths, keys - distribution, public and private.

Outcome 2

This Outcome introduces candidates to internet security options. It is not expected that candidates change these options, but candidates should recognise the security that is in place and should understand the level of security that is in place and determine whether it is appropriate.

Candidates should use encryption to send and receive e-mail. Candidates should be aware that e-mail sent as plain text is vulnerable and encryption can be applied to 'scramble' the message so that it can only be read by using the correct key to 'un-scramble' the message. Any suitable encryption software can be used for this task.

Outcome 3

In Outcome 3 candidates are required to use the internet or other suitable information source to gather information about internet security risks and how they can be resolved. Internet security is a major concern for users and new risks are appearing on a very regular basis. Candidates should be encouraged to research a topic of their choice which must be agreed in advance with the assessor. The topic to be researched should be sufficiently complex at this level as the candidate will be expected to possess a high level of skills for searching for information on the internet. Suitable topics may include phishing, virus, Denial of Service (DoS) etc.

This Outcome will introduce candidates to a method of presenting information for use with online communications. Candidates are required to present the researched information in an appropriate online format. It is expected that most centres will encourage candidates to produce a series of web pages using HTML. There is no prescribed format, centres may wish to use mobile phones and Wireless Mark-up Language (WML) or podcasting or video casting.

The range of features to be used will depend very much on the type of application chosen. If HTML is used the range of features would include hyperlinks to internal content within the same page, other pages within the site and external links, images with alternative text, appropriate layout methods such as tables and bulleted lists, suitable use of fonts etc. Candidates should be encouraged to demonstrate accessibility awareness within their published content wherever possible.

GUIDANCE ON LEARNING AND TEACHING APPROACHES FOR THIS UNIT

In Outcome 1 candidates will be introduced to a wide range of issues effecting complex online communications. It is expected that candidates will be assessed on computer based online communications methods and most of the teaching will be centred round this. If time permits, candidates may be introduced to other communications methods such as mobile phones that can be used for internet browsing, e-mail and downloads.

National Unit Specification: support notes (cont)

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

Candidates should be aware of the importance of open systems communications models. The model used in this Unit is TCP/IP but the International Standards Organisation Open Systems Interconnection (ISO OSI) model may also be introduced for comparison.

This Unit introduces candidates to some of the more complex security issues surrounding the internet. Outcome 3 involves the candidate carrying out research into a range of security issues and presenting this in an appropriate communications format. It is expected that time will be required to allow the candidate to develop skills in order to produce the presentation. The presentation may be

produced using HTML for web pages, WML for production on a mobile phone or may be produced using podcasting or video podcasting or any other appropriate online communication format.

The candidate may also carry out research into different types of encryption, including free applications, and they can select an appropriate application for use in Outcome 2.

A variety of freely available encryption software is available on the internet.

It is suggested that Outcome 1 be assessed at the end of the Unit as the candidate will gain knowledge through the research carried out in the practical activities.

The actual distribution of time between Outcomes is at the discretion of the centre, however one possible distribution of time is:

Outcome 1	14 hours
Outcome 2	4 hours
Outcome 3	22 hours

The allocated timings allow for assessment and re-assessment where required.

National Unit Specification: support notes (cont)

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

OPPORTUNITIES FOR CORE SKILL DEVELOPMENT

This Unit involves candidates using a range of IT facilities for searching and evaluating information which may provide opportunities to gather evidence for the IT and Problem Solving Core Skills. The published content may also provide opportunities to gather evidence for the Communications Core Skill.

GUIDANCE ON APPROACHES TO ASSESSMENT FOR THIS UNIT

It may be appropriate for some of the evidence for this Unit to be produced using e-assessment provided the national standard is applied and the conditions of assessment are consistent for all candidates. This may take the form of e-testing (for knowledge and understanding) and/or e-portfolios (for practical abilities).

If a centre is presenting Outcome 1 of these assessments online the following assessment methods, where appropriate, may be selected:

- Multiple choice
- Drag and drop
- Multiple response
- Mix and match
- a combination of the above

It is expected that the questions will be of the multiple-choice variety. Centres may consider the use of alternative questions types, particularly if using Computer Assisted Assessment approaches. However, care should be taken that the questions are valid and at an appropriate level. The use of simple true/false question responses is unlikely to achieve this.

The Assessment Support Pack for this Unit provides sample assessment material. Centres wishing to develop their own assessments should refer to the Assessment Support Pack to ensure a comparable standard.

For Outcome 1 a suitable assessment would be an objective test which demonstrates that the candidate has the required knowledge. The evidence for this Outcome should be obtained under controlled, supervised conditions. The assessment will be closed-book. Achievement can be decided by the use of a cut-off score.

Where re-assessment of knowledge and understanding is required the questions presented to the candidate must be different on each assessment occasion.

There is an opportunity to use an online assessment environment for knowledge and understanding of Outcome 1.

National Unit Specification: support notes (cont)

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

The assessment of practical skills throughout this Unit may be demonstrated in the context of a single extended task, or in the context of a number of smaller tasks. The candidate will normally demonstrate the skills during the teaching and learning activities of the Unit, rather than as separate assessment activities.

For the e-mail assessment the assessor could send the candidate an encrypted e-mail requesting a response, also encrypted, or the answer to a simple question. In order for the candidate to get the request for the response, or the question the candidate will require to decrypt the message thus providing evidence that the e-mail has been decrypted.

The research and content for Outcome 3 may be based on a single project relating to a security issue of the candidate's choice. This may be based on a topic that is currently in the news or one that the candidate has personally experienced.

This evidence material generated by this Unit may be stored in paper or electronic format.

If this Unit is undertaken in the workplace there may be opportunities for candidates to gather evidence in day to day workplace activities.

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 e-checklists. 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).*

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 alternative Outcomes for Units. Further advice can be found in the SQA document *Guidance on Assessment Arrangements for Candidates with Disabilities and/or Additional Support Needs* **(www.sqa.org.uk)**.

National Unit Specification: support notes (cont)

UNIT PC Passport: Working with Internet and Online Communications (SCQF level 6)

History of changes:

Version	Description of change	Date
02	Evidence Requirements clarified and/or details of NOS mapping inserted	10/08/2010