National Unit specification: general information

Unit title: Mobile Technology: Security and Peripherals (SCQF level 6)

Unit code: H2PB 12

Superclass: CC

Publication date: October 2012

Source: Scottish Qualifications Authority

Version: 01

Summary

This Unit develops knowledge and understanding of the principles of security related to mobile devices and the connectivity of peripherals. Candidates will develop practical skills in relation to connectivity through the use of contemporary mobile devices. The knowledge, understanding and practical skills developed will be applied by candidates to solve problems related to device connectivity.

This is a mandatory Unit in the National Progression Award (NPA) in Mobile Technology (SCQF level 6) and National Certificate (NC) in Mobile Technology (SCQF level 5), but is also available as a freestanding Unit.

Outcomes

1 Describe security issues and terminology associated with mobile technology.
2 Identify and use a range of security related applications for mobile devices.
3 Perform a back-up and restore of data from a mobile device.
4 Connect and configure mobile devices to operate a range of mobile peripherals.

Recommended entry

While entry is at the discretion of the centre, it would be beneficial if candidates have achieved one of the following, or equivalent:

H1T1 11 *Mobile Technology Systems*
FW02 11 *Computer Systems Architecture*

General information (cont)

Unit title: Mobile Technology: Security and Peripherals (SCQF level 6)

Credit points and level

1 National Unit credit at SCQF level 6: (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

Opportunities to develop aspects of Core Skills are highlighted in the support notes of this Unit specification.

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

National Unit specification: statement of standards

Unit title: Mobile Technology: Security and Peripherals (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

Describe security issues and terminology associated with mobile technology.

Performance Criteria

(a) Describe mobile device security concepts and terminology.
(b) Describe mobile device security threats.
(c) Describe steps that can be taken to mitigate security threats.

Outcome 2

Identify and use a range of security related applications for mobile devices.

Performance Criteria

(a) Identify utility applications that allow security enhancements on mobile devices.
(b) Install and correctly configure security based utility applications.

Outcome 3

Perform a back-up and restore of data from a mobile device.

Performance Criteria

(a) Identify back-up solutions for a range of mobile devices.
(b) Back-up prescribed data from a mobile device.
(c) Restore prescribed data to a mobile device.

Outcome 4

Connect and configure mobile devices to operate a range of mobile peripherals.

Performance Criteria

(a) Configure a mobile device to accept peripheral connections.
(b) Configure and connect mobile device peripherals using wireless methods.
(c) Configure and connect mobile device peripherals using wired methods.

National Unit specification: statement of standards (cont)

Unit title: Mobile Technology: Security and Peripherals (SCQF level 6))

Evidence Requirements for this Unit

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

Outcome 1

For Outcome 1, written and/or oral evidence generated under closed-book conditions, is required which demonstrates that candidates can:

- describe a minimum of three mobile device security concepts and a minimum of three mobile device security terms
- describe a minimum of three mobile device security threats
- describe steps that can be taken to mitigate security threats

Outcome 2

For Outcome 2, written and/or oral and performance evidence generated under open-book conditions is required, which demonstrates that candidates can:

- identify the required utility applications for a given scenario and outline their relevance to the security enhancement on a mobile device
- install and correctly configure two security utility applications for a given scenario

Outcome 3

For Outcome 3, written and/or oral and performance evidence generated under open-book conditions is required, which demonstrates that candidates can:

- identify back-up solutions for at least two types of mobile device
- back-up prescribed data from a mobile device
- restore prescribed data to a mobile device

Outcome 4

For Outcome 4, performance evidence generated under open-book conditions is required, which demonstrates that candidates can:

- configure a mobile device to accept peripheral connections
- configure and connect two mobile device peripherals using wireless methods
- configure and connect two mobile device peripherals using wired methods

National Unit specification: support notes

Unit title: Mobile Technology: Security and Peripherals (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

The Unit centres on the two main areas of security of mobile devices, and the connection of peripheral devices to mobile devices.

The aim of Outcome 1 is to lay the foundation of knowledge of the security threats that may be encountered when using a mobile device. Traditional thinking centres on the computer system, but as mobile devices become increasingly complex and hold more data, security is increasingly important on these devices. Security threats may be in the form of malware and spyware applications, Wi-Fi threats, lost or stolen devices or communication interception.

Security mitigation may come in the form of a trusted anti-malware solution, personal firewall solution or robust password protection to protect device access.

Outcome 2 looks at the installation of software or applications based on a given scenario (but there should be sufficient scope during the Outcome to consider many scenarios). The scenario given to candidates must be a real-world example. Candidates should be given the scenario and then outline a potential application that would suit the needs in the scenario. The next phase is to install and correctly configure two security applications, for a given scenario. These may or may not be the same as those identified in the first part of the Outcome. These may be downloaded from an application 'store' or be pieces of software that are held locally.

Outcome 3 looks at the back-up solutions that exist for mobile devices. As more data is being stored on mobile devices such as music, e-mails, documents, photographs, calendar entries, etc there is a need to perform back-up and restore of this type of data. The Outcome should look at the types of back-up that exist, such as local and cloud storage, and the methods for carrying out a back-up and restore. The practical element for candidates is to perform a back-up and restore of prescribed data to/from a mobile device.

Outcome 4 covers the increased use of peripherals with mobile devices. Such peripherals include Bluetooth headsets, and output devices such as printers, speakers and video devices. Peripheral input devices include keyboards, tablets, mice, and musical instruments. The Outcome should cover common wired and wireless types of connection.

National Unit specification: support notes (cont)

Unit title: Mobile Technology: Security and Peripherals (SCQF level 6)

Guidance on learning and teaching approaches for this Unit

The types of devices or connections to be used are not specified, which allows teaching to be carried out on any appropriate contemporary devices. In the main, this may be mobile phones but delivery could focus on such items as portable tablet devices.

Outcome 1 — concentrates on the foundation of the security threats that may be encountered when using a mobile device, therefore learning and teaching should focus not on the computer system, but on the mobile devices.

As far as possible, the topics should be delivered in such a way that the practical uses and implications of the subject are made clear to candidates.

For this part of the Unit the tutor should concentrate on two key aspects of the threat towards security of mobile devices:

- security threats may come in the form of malware and spyware applications, Wi-Fi threats, lost or stolen devices, communication interception
- security mitigation may come in the form of a trusted anti-malware solution, personal firewall solution or robust password protection to protect device access

Outcome 2 — looks at the installation of software or applications for mobile devices, therefore the learning and teaching should focus on practical situations supported by theory to enhance candidates' knowledge and understanding.

Outcome 3 — is based on the back-up solutions that exist for mobile devices and candidates are expected to be able to develop skills in performing a back-up and restore of prescribed data to/from a mobile device. Therefore, the learning and teaching should focus on practical situations supported by theory to enhance candidates' knowledge and understanding.

Outcome 4 — is based on the increased use of peripherals with mobile devices and candidates will develop skills in the configuration and connection of common wired and wireless types of devices. Therefore, the learning and teaching should focus on practical situations supported by theory to enhance the candidates' knowledge and understanding.

Guidance on approaches to assessment for this Unit

Assessment for Outcome 1 should be in the form of appropriate questioning methods that will reinforce the candidate's experience.

Outcomes 2, 3 and 4 should utilise the blended approach of theory and practical based assignments. It is intended that these Outcomes are delivered individually, but they could be integrated where it is of benefit to centres and to candidates.

National Unit specification: support notes (cont)

Unit title: Mobile Technology: Security and Peripherals (SCQF level 6)

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)*.

Opportunities for developing Core Skills

In this Unit candidates are required to use a range of features provided by software application packages and utilise mobile devices which provides opportunities to develop aspects of the Core Skill of *Information and Communication Technology*.

In Outcomes 2, 3 and 4, candidates will be assigned specific tasks that will require a certain level of planning and critical thinking which provides opportunities to develop aspects of the Core Skill of *Problem Solving*.

Written and/oral reporting in any practical exercises and assessments may provide opportunities to develop aspects of the Core Skill of *Communication*.

The nature of some specific applications may provide opportunities to develop aspects of the Core Skill of *Numeracy*.

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