



F0H5 10 - Internet Safety (Intermediate 1)

Delivery Guide

Version 2.0

Publication Date: January 2009

The information in this publication may be reproduced to support SQA qualifications. If it is reproduced, SQA should be clearly acknowledged as the source. If it is to be used for any other purpose, then written permission must be obtained from the Support Materials Development Officer at SQA. It must not be reproduced for trade or commercial purposes.

CONTENTS PAGE

1. Purpose of guide	3
Background to project.....	3
Aims of the project.....	3
Who the unit is for	4
Who this guide is for.....	4
What this guide aims to do.....	4
Links with other units	4
Sources of support.....	4
2. Overview of unit	5
Outcomes	5
Assessment.....	6
3 Resources Available	7
Teaching and Learning Materials	7
Online.....	7
Moodle	7
Mobile.....	7
Online assessment.....	7
Selection of blogging software	7
4. Teacher Led Delivery	8
Resources required.....	8
Use of Teaching & Learning material	8
Delivery models	8
Whole class groups	8
Mixed classes	8
Assessment.....	8
Teaching plan.....	8
5. Student centred	19
Resources required.....	19
Use of Teaching & Learning material	19
Learning strategies	19
Assessment.....	19
Learning plan	19
6. E-learning (self taught)	30
Resources required.....	30
Use of Teaching & Learning material	30
Learning strategies	30
Sources of support.....	30
Assessment.....	30
Learning plan	30
7. Delivery issues	41
Teaching and Learning Materials	41
Online.....	41
Moodle	41
Mobile.....	41
Assessment.....	41
Authentication.....	41
Re-assessment	41
Formative assessment	41
Online assessment.....	42
Selection of blogging software	42

1. PURPOSE OF GUIDE

Background to project

Internet safety is about the safe and legal use of the Internet. The Internet is used by lots of people – of all ages – for lots of purposes, ranging from chatting to friends to booking a holiday – and the use of the ‘Net is growing at a rapid pace. But there are risks involved in using the Internet. These risks include: unwanted e-mail, online fraud, identity theft, child grooming and viruses. There are numerous media reports about abuses. And new threats are emerging all of the time. A large survey carried out by Ofcom highlighted these two trends – growing use of the Internet, accompanied by increased threats to personal safety – and emphasised the lack of awareness about potential threats.

So Internet safety means knowing about potential threats when you are online; knowing what you can and cannot (legally) do when you are online; and knowing how to protect yourself from some of the risks that are involved in using the ‘Net.

There are already lots of short courses available on Internet safety, so why the need for a formal qualification? SQA carried out research among centres and over 90% of teachers reported an interest in offering such a qualification. The survey made two things clear: (1) teachers and lecturers were concerned about Internet safety; and (2) most centres only offered *ad hoc* advice to pupils and students on how to protect themselves.

So it was felt that a qualification would formalise the approach to Internet safety and standardise the advice given to students. And since it’s a National Qualification, schools and colleges would be funded to deliver it.

We think that it’s the first national qualification in Internet safety in the world. We’re hoping that it will appeal to international students and make a contribution to improving the safety of students in lots of countries.

Aims of the project

The qualification is very straight-forward. It consists of a **single** National Unit at **SCQF level 4** (Intermediate 1). The unit is entitled: “Internet Safety”. There are **four outcomes** in the Unit:

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.

The unit specification is available on the SQA website (<http://www.sqa.org.uk>)

The threats covered include identity theft, cyber-bullying, grooming, phishing and pharming (Outcome 1). Advice is provided on how best to combat these threats (Outcome 2) such as how to set-up virus protection and firewalls, and how to recognise an online scam. The unit also explains your legal responsibilities when using the Internet (Outcome 3) and discusses issues such as copyright restrictions on downloading music. The final outcome puts all of this into practice by ensuring that students can actually take precautions and work safely online.

This qualification is SQA’s first “e-only” qualification – in other words, the first qualification that is **only** available online. SQA normally produces a range of paper-based support material for new qualifications but this qualification will be supported with digital material – there will be no paper material. So, the teaching and learning material will be in digital format and the assessments will be available online.

Who the unit is for

The unit should be of interest to anyone who uses the Internet. Although much of the media focus is on young people, mature users are just as likely to experience problems. So the unit is designed for school pupils, college students, adults who work with children, people who shop online, and “silver surfers”. It is expected that the unit will also be of particular interest to practicing teachers and librarians who may want to know more about the potential dangers facing young people in their charge.

Who this guide is for

This guide is intended principally for the use of teachers and tutors delivering the unit or supporting candidates who are studying it on their own. It gives guidance on delivering the unit on a teacher-centred, student centred or e-learning (self-taught) basis. Parts of it may also be of interest to candidates, particularly those who are studying independently.

What this guide aims to do

This guide aims to provide teachers with the information required to deliver the unit successfully in a teacher-led or student centred delivery context. It gives advice regarding the scheduling of the material and information about sources of additional resources. It should also be of use to self-taught candidates who are studying the unit via e-learning.

Links with other units

This unit can usefully be delivered in parallel with the NQ Unit DN81 11: Weblogs (Intermediate 2). If a Weblog is used as a means of recording the candidate’s completion of the practical assessments for the Internet Safety units it can also serve as assessment evidence for the Weblogs unit.

Sources of support

Centres requiring additional support should contact ict@sqa.org.uk in the first instance.

2. OVERVIEW OF UNIT

Outcomes

1. Identify threats that can exist when using the Internet.

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 these categories.

They 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 of all these categories.

Candidates should know that threats to user safety include abusive behaviour, inappropriate behaviour and grooming. They should be aware that these threats can appear in a variety of different contexts, eg chat rooms, e-mail or instant messaging.

2. Describe safety precautions which should be taken when using the Internet.

Candidates must be aware that precautions for maintaining system performance and integrity include firewalls, software for detecting and disabling malicious programs (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 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 know that precautions for maintaining data security include firewalls, software for detecting and disabling malicious programs (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 suites, 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.

Candidates should know 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.

3. Describe legal constraints which apply when using the Internet.

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.

They 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. 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.

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

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).

They should know 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). They should also know that precautions for maintaining user safety include content filtering, proxy servers, monitoring and reporting user behaviour and withholding personal information.

Candidates should be aware that copyright restrictions must always be taken into consideration when downloading content.

Assessment

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 is an assessment consisting of 25 multiple choice questions which assess candidates’ knowledge and understanding. It is expected 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 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).

3 RESOURCES AVAILABLE

Teaching and Learning Materials

SQA have produced comprehensive learning and teaching resources which are available in various formats:

Online

An online version of the teaching and learning materials is available at <http://www.sqasolar.org.uk>

Moodle

A version of the materials hosted in SQA's Moodle VLE (Virtual Learning Environment) is available at <http://www.myqualifications.com>

Mobile

A version of the Teaching and Learning materials that is ideal for those accessing them from a mobile phone or similar device with a small screen is available at <http://e-learning-computing.com/mobile>

Online assessment

The knowledge assessment can easily be assessed online through SQA's e-assessment engine, called SOLAR. Solar can be used for summative assessments and can be used by teachers and lecturers to create formative and practice assessments.

If you are a Scottish FE college you can currently access the knowledge assessment in Solar. If you are another SQA centre and would also like to use the online assessment through Solar, then please contact the Solar Team on solar@sqa.org.uk

Visit the Solar website <http://www.sqasolar.org.uk> to see when we are next holding training events.

Selection of blogging software

Almost any blogging tool can be used to create a weblog for assessment purposes. Centres will probably find it easier to use a hosted service rather than install blogging software themselves. Information about a number of suitable services can be found at: http://en.wikibooks.org/wiki/Weblogs#Weblog_providers

4. TEACHER LED DELIVERY

Resources required

Candidates will require access to the online learning materials provided by SQA. Ideally they should also have live Internet access during teaching sessions, so that links in the teaching material can be followed, and (where permitted) additional resources downloaded. If candidates are using a blog to keep a log of practical assessment tasks completed then access to blogging software will also be required.

Use of Teaching & Learning material

The teaching and learning material can be accessed in the following formats:

- ONLINE <http://www.sqasolar.org.uk/mini/27622.1198.1318.html>
- MOODLE <http://www.myqualifications.com>
- MOBILE <http://e-learning-computing.com/mobile>

Delivery models

Whole class groups

The teaching plan given overleaf should be suitable for use with whole-class groups.

Mixed classes

The teaching plan given overleaf may require to be adapted for use with mixed groups. In particular, some students may need time to progress through the lessons at a slower pace, or need additional time at the end of each section for review and assessment.

Assessment

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 takes 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 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).

Teaching plan

It is recommended that the course material should be delivered by means of **thirty lessons**, each of which will involve reading the relevant online materials (including following links, where appropriate) and completion of any quizzes.

Section 1: Viruses

Lesson 1:

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Introduction
- Viruses, Trojans and Worms
- Types of Virus
- Trojans
- Virus Quiz 1

The lesson should end with a brief review of the relevant points, eg:

- Relatively recent origin of computer threats
- Risk to all types of machines
- Virus payloads
- Different types of virus:
 - File infector viruses
 - Boot sector viruses
 - Multi-partite viruses
 - Macro viruses
- Characteristics of Trojans

Lesson 2:

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Worms
- Logic Bombs and Other Threats
- Virus Quiz 2
- Screen Savers
- Image Viruses
- Virus Quiz 3

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of worms
- Characteristics of logic bombs etc
- Characteristics of screen saver viruses
- Characteristics of image viruses

Lesson 3:

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Macro Virus
- Resident Virus
- Virus Quiz 4
- Script Viruses
- Stealth Viruses
- Virus Quiz 5

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of macro viruses
- Characteristics of resident viruses
- Characteristics of script viruses
- Characteristics of stealth viruses

Lesson 4:

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Mail Bombs
- Backdoor (or Rootkit) Viruses
- Virus Quiz 6

Rootkits are likely to be of particular interest to students due to the involvement of a major record company. It may be useful to hold a brief class discussion on this stage on the conflict between a record company taking steps to protect its rights and the right of consumers not to have their machines infected. Additional information can be found at the following locations:

<http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx>

<http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx>

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of mail bombs
- Characteristics of backdoor / rootkit viruses

Lesson 5:

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. The importance of installing Anti-Virus software on home machines should be emphasised.

- Example Viruses
- Anti-Virus Software
- How Anti-Virus Software Works

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Anti-Virus software

Lesson 6

This lesson does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Viruses
- Completion of log

Depending on the facilities available locally, the activities recorded in the log should be either:

1. Details of the installation of an anti-virus package by the student. If local restrictions prevent the installation of an Anti-Virus package, it may be possible to install a package on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
2. Comparison of the features offered by three different Anti-Virus packages. The information required to carry out the comparison can be obtained from the web sites of the relevant Anti-Virus software suppliers.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Lesson 7

This session should be used to finish completing the log for this topic.

Section 2: Malicious Software (Malware)

Lesson 8

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Introduction
- Spyware
- Drive-By-Downloads
- Dealing with Spyware
- Spyware Clues
- Spyware Quiz1
- Spyware SQA2

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Spyware
- Dealing with Spyware

Lesson 9

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. The importance of installing Anti-Spyware software should be emphasised.

- How Anti Spyware Software Works
- Adware
- Adware – Read the Small Print
- Dealing with Adware
- Adware Quiz

The lesson should end with a brief review of the relevant points, eg:

- Anti/Spyware Software
- Characteristics of Adware
- Dealing with Adware

Lesson 10

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. The dangers posed by Rogue Diallers to users of DialUp connections should be emphasised.

- Key Loggers
- Rogue Diallers
- DOS Attack
- Internet Threats Quiz

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Key Loggers
- Characteristics of Rogue Diallers
- Characteristics of DOS Attacks

Lesson 11

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. The importance of Spam Filters and Anti-Spam Software should be emphasised.

- Spam
- How Spammers Work
- Spam Filters
- Anti Spam Software
- Spam Quiz 1
- Spam Quiz 2

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Spam
- Spam Filters and Anti-Spam Software

Lesson 12

This lesson does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Malware
- Completion of log

Depending on the facilities available locally, the activities recorded in the log should be either:

1. Details of the installation of anti-spam and anti-spyware by the student. If local restrictions prevent the installation of relevant packages, it may be possible to install packages on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
2. Comparison of the features offered by three different anti-spam packages and three different anti-spyware packages. The information required to carry out the comparisons can be obtained from the web sites of the relevant software suppliers.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Lesson 13

This session should be used to finish completing the log for this topic.

Section 3: Other Internet Threats

Lesson 14

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. It should be emphasised that genuine financial institutions will never ask for personal details to be submitted by email.

- Phishing
- Phishing Scam
- How to Defend Against Phishing
- Phishing Quiz

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Phishing
- Defences Against Phishing

Lesson 15

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Identity Theft
- Identity Theft Quiz
- Hoaxes
- Virus Hoaxes
- Hoax Activity
- Hoax Quiz

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Identity Theft
- Characteristics of Hoaxes

Lesson 16

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Ransomware
- Ransomware Quiz
- Hackers
- Hacker Activity
- Internet Threats Quiz 2

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Ransomware
- Characteristics of Hacking

Lesson 17

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. It should be emphasised that any suspected instances of Cyberbullying or Grooming should always be reported to a responsible adult.

- Cyberbullying
- Tackling Cyberbullying

- Internet Grooming
- How to Protect Yourself
- Internet Threats Quiz 3

Grooming is a very sensitive topic, so the online materials in this area have been deliberately kept very low key in order to allow teachers maximum discretion as to the level at which they wish to tackle this topic, in keeping with local circumstances. For those who wish to go into greater depth, useful material can be found at:

<http://www.uclan.ac.uk/host/cru/docs/NewCyberStalking.pdf#search=%22lancashire%20grooming%22>

The lesson should end with a brief review of the relevant points, eg:

- Characteristics of Cyberbullying
- Characteristics of Grooming
- Protection against Cyberbullying and Grooming

Lesson 18

This lesson does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Other Internet Threats
- Completion of Log

The log should give details of the steps taken by the student to protect himself / herself against Internet threats such as Phishing, Identity Theft, Hackers, Cyberbullying and Grooming.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Section 4: Internet Defences

Lesson 19

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes.

- Introduction
- Internet Defence Activity
- Avoiding Threats
- Removing Threats
- Internet Security Suites

The lesson should end with a brief review of the relevant points, eg:

- Internet Defence Activity
- Avoiding and Removing Threats
- Internet Security Suites

Lesson 20

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. The importance of using strong passwords and keeping passwords secret should be emphasised.

- Passwords
- Password Security
- Password Security Activity
- Passwords Quiz 1
- Passwords Quiz 2

The lesson should end with a brief review of the relevant points, eg:

- Passwords
- Password Security

Lesson 21

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. The importance of using Firewalls and Content Filtering software on home machines, and backing up critical files regularly should be emphasised.

- Firewalls
- Firewall Quiz
- Proxy Servers
- Content Filtering
- Backup/Restore
- Internet Defences Quiz

The lesson should end with a brief review of the relevant points, eg:

- Firewalls
- Proxy Servers
- Content Filtering
- Backup/Restore

Lesson 22

This lesson does not make use of the online materials. Instead, it should concentrate on the following areas:

- Internet Defences Review
- Completion of Log

Depending on the facilities available locally, the activities recorded in the log should be either:

1. Details of the installation of firewall, content filtering and internet security software by the student. If local restrictions prevent the installation of relevant packages, it may be possible to install packages on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
2. Comparison of the features offered by two different firewall packages, two different content-filtering packages and two different internet security suites. The information required to carry out the comparisons can be obtained from the web sites of the relevant software suppliers.

The log should also give details of the steps taken by the student to generate secure passwords and backup and restore critical files. It should not contain examples of genuine passwords.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Lesson 23

This session should be used to finish completing the log for this topic.

Section 5: Legal Aspects

Lesson 24

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material and quizzes. Emphasis should be placed on the dubious legality of P2P and the possibility of both P2P software and downloaded files introducing malicious software into a system.

- Downloading Files
- Why You Should Avoid P2P
- Alternatives to P2P

The lesson should end with a brief review of the relevant points, eg:

- Dangers of P2P

Lesson 25

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material. The fact that the majority of information found on the Internet is likely to be copyright, and thus subject to restrictions on use, should be emphasised.

- Copyright
- Copyright and the Internet
- Digital Rights Management

The lesson should end with a brief review of the relevant points, eg:

- Copyright and the Internet
- Digital Rights Management

Lesson 26

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material. The importance of ensuring that websites are accessible to users with disabilities should be emphasised.

- Disability Discrimination Legislation
- The Data Protection Act

The lesson should end with a brief review of the relevant points, eg:

- Disability Discrimination Legislation
- The Data Protection Act

Lesson 27

Teachers should begin by introducing the day's topic briefly to students, then allowing them to work their way through the following online material. Candidates should be made aware that the considerations regarding chat rooms apply equally to Instant Messaging and Social Networking sites.

- Chat Rooms

The lesson should end with a brief review of the relevant points, eg:

- Chat Rooms

Lesson 28

This lesson does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Legal Aspects
- Completion of Log

The log should include details of the steps taken by the candidate to ensure that his/her own activities comply with all relevant legal requirements and safety recommendations, eg: detail of legal downloads made, steps taken to make websites accessible, steps taken to minimise display of personal information, etc.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Lesson 29

This lesson does not make use of the online materials. Instead, it should concentrate on the following areas:

- Course Review
- Final Completion of Logs

Any logs which need further attention should be completed at this stage, or arrangements made for their completion at some subsequent date.

Lesson 30

This session should be used to allow candidates to undertake the Online Assessment (MCQs). Arrangements should be made to allow candidates who do not complete this successfully to resit at a later date after appropriate remediation.

5. STUDENT CENTRED

Resources required

Candidates will require access to the online learning materials provided by SQA. Ideally they should also have live Internet access during teaching sessions, so that links in the teaching material can be followed, and (where permitted) additional resources downloaded. If candidates are using a blog to keep a log of practical assessment tasks completed then access to blogging software will also be required.

Use of Teaching & Learning material

The teaching and learning material can be accessed in the following formats:

- ONLINE <http://www.sgasolar.org.uk/mini/27622.1198.1318.html>
- MOODLE <http://www.myqualifications.com>
- MOBILE <http://e-learning-computing.com/mobile>

Learning strategies

The Learning Plan overleaf gives suggestions regarding appropriate Learning Strategies.

Assessment

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 takes 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 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).

Learning plan

It is recommended that the course material should be covered over **thirty sessions**, each of approximately one hour's duration. Each session will involve reading the relevant online materials (including following links, where appropriate) and completion of any quizzes.

Section 1: Viruses

Session 1:

Candidates should work their way through the following online material and quizzes.

- Introduction
- Viruses, Trojans and Worms
- Types of Virus
- Trojans
- Virus Quiz 1

The Session should end with a brief review of the relevant points, eg:

- Relatively recent origin of computer threats
- Risk to all types of machines
- Virus payloads
- Different types of virus:
 - File infector viruses
 - Boot sector viruses
 - Multi-partite viruses
 - Macro viruses
- Characteristics of Trojans

Session 2:

Candidates should work their way through the following online material and quizzes.

- Worms
- Logic Bombs and Other Threats
- Virus Quiz 2
- Screen Savers
- Image Viruses
- Virus Quiz 3

The Session should end with a brief review of the relevant points, eg:

- Characteristics of worms
- Characteristics of logic bombs etc.
- Characteristics of screen saver viruses
- Characteristics of image viruses

Session 3:

Candidates should work their way through the following online material and quizzes.

- Macro Virus
- Resident Virus
- Virus Quiz 4
- Script Viruses
- Stealth Viruses
- Virus Quiz 5

The Session should end with a brief review of the relevant points, eg:

- Characteristics of macro viruses
- Characteristics of resident viruses
- Characteristics of script viruses
- Characteristics of stealth viruses

Session 4:

Candidates should work their way through the following online material and quizzes.

- Mail Bombs
- Backdoor (or Rootkit) Viruses
- Virus Quiz 6

Candidates may find Rootkits to be of particular interest, due to the involvement of a major record company. It may be useful to consider or research the conflict between a record company taking steps to protect its rights and the right of consumers not to have their machines infected.

Additional information can be found at the following locations:

<http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx>

<http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx>

The Session should end with a brief review of the relevant points, eg:

- Characteristics of mail bombs
- Characteristics of backdoor / rootkit viruses

Session 5:

Candidates should work their way through the following online material and quizzes. The importance of installing Anti-Virus software on home machines should be noted.

- Example Viruses
- Anti-Virus Software
- How Anti-Virus Software Works

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Anti-Virus software

Session 6

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Viruses
- Completion of log

Depending on the facilities available locally, the activities recorded in the log should be either:

1. Details of the installation of an anti-virus package by the student. If local restrictions prevent the installation of an Anti-Virus package, it may be possible to install a package on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
2. Comparison of the features offered by three different Anti-Virus packages. The information required to carry out the comparison can be obtained from the web sites of the relevant Anti-Virus software suppliers.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 7

This session should be used to finish completing the log for this topic.

Section 2: Malicious Software (Malware)

Session 8

Candidates should work their way through the following online material and quizzes.

- Introduction
- Spyware
- Drive-By-Downloads
- Dealing with Spyware
- Spyware Clues
- Spyware Quiz1
- Spyware SQA2

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Spyware
- Dealing with Spyware

Session 9

Candidates should work their way through the following online material and quizzes. The importance of installing Anti-Spyware software should be noted.

- How Anti Spyware Software Works
- Adware
- Adware – Read the Small Print
- Dealing with Adware
- Adware Quiz

The Session should end with a brief review of the relevant points, eg:

- Anti/Spyware Software
- Characteristics of Adware
- Dealing with Adware

Session 10

Candidates should work their way through the following online material and quizzes. The dangers posed by Rogue Diallers to users of DialUp connections should be noted.

- Key Loggers
- Rogue Diallers
- DOS Attack
- Internet Threats Quiz

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Key Loggers
- Characteristics of Rogue Diallers
- Characteristics of DOS Attacks

Session 11

Candidates should work their way through the following online material and quizzes. The importance of Spam Filters and Anti-Spam Software should be noted.

- Spam
- How Spammers Work

- Spam Filters
- Anti Spam Software
- Spam Quiz 1
- Spam Quiz 2

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Spam
- Spam Filters and Anti-Spam Software

Session 12

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Malware
- Completion of log

Depending on the facilities available locally, the activities recorded in the log should be either:

1. Details of the installation of anti-spam and anti-spyware by the student. If local restrictions prevent the installation of relevant packages, it may be possible to install packages on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
2. Comparison of the features offered by three different anti-spam packages and three different anti-spyware packages. The information required to carry out the comparisons can be obtained from the web sites of the relevant software suppliers.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 13

This session should be used to finish completing the log for this topic.

Section 3: Other Internet Threats

Session 14

Candidates should work their way through the following online material and quizzes. They should know that genuine financial institutions will never ask for personal details to be submitted by email.

- Phishing
- Phishing Scam
- How to Defend Against Phishing
- Phishing Quiz

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Phishing
- Defences Against Phishing

Session 15

Candidates should work their way through the following online material and quizzes.

- Identity Theft
- Identity Theft Quiz
- Hoaxes
- Virus Hoaxes
- Hoax Activity
- Hoax Quiz

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Identity Theft
- Characteristics of Hoaxes

Session 16

Candidates should work their way through the following online material and quizzes.

- Ransomware
- Ransomware Quiz
- Hackers
- Hacker Activity
- Internet Threats Quiz 2

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Ransomware
- Characteristics of Hacking

Session 17

Candidates should work their way through the following online material and quizzes. They should be aware that any suspected instances of Cyberbullying or Grooming should always be reported to a responsible adult.

- Cyberbullying
- Tackling Cyberbullying
- Internet Grooming
- How to Protect Yourself
- Internet Threats Quiz 3

Grooming is a very sensitive topic, so the online materials in this area have been deliberately kept very low key. For those who wish to go into greater depth, useful material can be found at:

<http://www.uclan.ac.uk/host/cru/docs/NewCyberStalking.pdf#search=%22lancashire%20grooming%22>

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Cyberbullying
- Characteristics of Grooming
- Protection against Cyberbullying and Grooming

Session 18

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Other Internet Threats
- Completion of Log

The log should give details of the steps taken by the student to protect himself / herself against Internet threats such as Phishing, Identity Theft, Hackers, Cyberbullying and Grooming.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Section 4: Internet Defences

Session 19

Candidates should work their way through the following online material and quizzes.

- Introduction
- Internet Defence Activity
- Avoiding Threats
- Removing Threats
- Internet Security Suites

The Session should end with a brief review of the relevant points, eg:

- Internet Defence Activity
- Avoiding and Removing Threats
- Internet Security Suites

Session 20

Candidates should work their way through the following online material and quizzes. They should recognise the importance of using strong passwords and keeping passwords secret.

- Passwords
- Password Security
- Password Security Activity
- Passwords Quiz 1
- Passwords Quiz 2

The Session should end with a brief review of the relevant points, eg:

- Passwords
- Password Security

Session 21

Candidates should work their way through the following online material and quizzes. They should be aware of the importance of using Firewalls and Content Filtering software on home machines, and backing up critical files regularly.

- Firewalls
- Firewall Quiz
- Proxy Servers
- Content Filtering
- Backup/Restore
- Internet Defences Quiz

The Session should end with a brief review of the relevant points, eg:

- Firewalls
- Proxy Servers
- Content Filtering
- Backup/Restore

Session 22

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Internet Defences Review
- Completion of Log

Depending on the facilities available locally, the activities recorded in the log should be either:

1. Details of the installation of firewall, content filtering and internet security software by the student. If local restrictions prevent the installation of relevant packages, it may be possible to install packages on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
2. Comparison of the features offered by two different firewall packages and two different content-filtering packages and two different internet security suites. The information required to carry out the comparisons can be obtained from the web sites of the relevant software suppliers.

The log should also give details of the steps taken by the student to generate secure passwords and backup and restore critical files. It should not contain examples of genuine passwords.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 23

This session should be used to finish completing the log for this topic.

Section 5: Legal Aspects

Session 24

Candidates should work their way through the following online material and quizzes. They should be aware of the dubious legality of P2P and the possibility of both P2P software and downloaded files introducing malicious software into a system.

- Downloading Files
- Why You Should Avoid P2P
- Alternatives to P2P

The Session should end with a brief review of the relevant points, eg:

- Dangers of P2P

Session 25

Candidates should work their way through the following online material. They should realize that the majority of information found on the Internet is likely to be copyright, and thus subject to restrictions on use.

- Copyright
- Copyright and the Internet
- Digital Rights Management

The Session should end with a brief review of the relevant points, eg:

- Copyright and the Internet
- Digital Rights Management

Session 26

Candidates should work their way through the following online material. They should realize the importance of ensuring that websites are accessible to users with disabilities.

- Disability Discrimination Legislation
- The Data Protection Act

The Session should end with a brief review of the relevant points, eg:

- Disability Discrimination Legislation
- The Data Protection Act

Session 27

Candidates should work their way through the following online material. They should be aware that the considerations regarding chat rooms apply equally to Instant Messaging and Social Networking sites.

- Chat Rooms

The Session should end with a brief review of the relevant points, eg:

- Chat Rooms

Session 28

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Legal Aspects
- Completion of Log

The log should include details of the steps taken by the candidate to ensure that his/her own activities comply with all relevant legal requirements and safety recommendations, eg: detail of legal downloads made, steps taken to make websites accessible, steps taken to minimise display of personal information, etc.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 29

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Course Review
- Final Completion of Logs

Any logs which need further attention should be completed at this stage, or arrangements made for their completion at some subsequent date.

Session 30

This session should be used to allow candidates to undertake the Online Assessment (MCQs). Arrangements should be made to allow candidates who do not complete this successfully to resit at a later date after appropriate remediation.

6. E-LEARNING (SELF TAUGHT)

Resources required

Candidates will require access to the online learning materials provided by SQA. Ideally they should also have live Internet access during teaching sessions, so that links in the teaching material can be followed, and (where permitted) additional resources downloaded. If candidates are using a blog to keep a log of practical assessment tasks completed then access to blogging software will also be required.

Use of Teaching & Learning material

The teaching and learning material can be accessed in the following formats:

- ONLINE <http://www.sqasolar.org.uk/mini/27622.1198.1318.html>
- MOODLE <http://www.myqualifications.com>
- MOBILE <http://e-learning-computing.com/mobile>

Learning strategies

The Learning Plan given overleaf suggests appropriate learning strategies.

Sources of support

Your first-line source of support should be the tutor allocated to you by the centre where you have enrolled for the unit.

Assessment

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 takes 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 you have had an opportunity to acquire the essential knowledge and understanding required to give you a realistic prospect to pass the assessment.

The assessment for Outcome 4 is a practical assessment consisting of observation of your activity over an extended period of time during which you are required to maintain a log of activity. It is recommended that this assessment is started at the earliest opportunity, as soon as you have acquired the necessary knowledge and skills to permit you to commence appropriate tasks.

The assessment for this Unit is well-suited to online assessment. The assessment of knowledge and understanding (Outcomes 1-3 will be assessed using an item bank of appropriate questions; and the assessment of practical abilities (Outcome 4) will be assessed using a digital repository for your log (such as an e-portfolio or web log).

Learning plan

It is recommended that the course material should be covered over **thirty sessions**, each of approximately one hour's duration. Each session will involve reading the relevant online materials (including following links, where appropriate) and completion of any quizzes.

Section 1: Viruses

Session 1:

Candidates should work their way through the following online material and quizzes.

- Introduction
- Viruses, Trojans and Worms
- Types of Virus
- Trojans
- Virus Quiz 1

The Session should end with a brief review of the relevant points, eg:

- Relatively recent origin of computer threats
- Risk to all types of machines
- Virus payloads
- Different types of virus:
 - File infector viruses
 - Boot sector viruses
 - Multi-partite viruses
 - Macro viruses
- Characteristics of Trojans

Session 2:

Candidates should work their way through the following online material and quizzes.

- Worms
- Logic Bombs and Other Threats
- Virus Quiz 2
- Screen Savers
- Image Viruses
- Virus Quiz 3

The Session should end with a brief review of the relevant points, eg:

- Characteristics of worms
- Characteristics of logic bombs etc.
- Characteristics of screen saver viruses
- Characteristics of image viruses

Session 3:

Candidates should work their way through the following online material and quizzes.

- Macro Virus
- Resident Virus
- Virus Quiz 4
- Script Viruses
- Stealth Viruses
- Virus Quiz 5

The Session should end with a brief review of the relevant points, eg:

- Characteristics of macro viruses
- Characteristics of resident viruses
- Characteristics of script viruses
- Characteristics of stealth viruses

Session 4:

Candidates should work their way through the following online material and quizzes.

- Mail Bombs
- Backdoor (or Rootkit) Viruses
- Virus Quiz 6

Candidates may find Rootkits to be of particular interest, due to the involvement of a major record company. It may be useful to consider or research the conflict between a record company taking steps to protect its rights and the right of consumers not to have their machines infected.

Additional information can be found at the following locations:

<http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx>

<http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx>

The Session should end with a brief review of the relevant points, eg:

- Characteristics of mail bombs
- Characteristics of backdoor / rootkit viruses

Session 5:

Candidates should work their way through the following online material and quizzes. The importance of installing Anti-Virus software on home machines should be noted.

- Example Viruses
- Anti-Virus Software
- How Anti-Virus Software Works

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Anti-Virus software

Session 6

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Viruses
- Completion of log

Depending on the facilities available locally, the activities recorded in the log should be either:

3. Details of the installation of an anti-virus package by the student. If local restrictions prevent the installation of an Anti-Virus package, it may be possible to install a package on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
4. Comparison of the features offered by three different Anti-Virus packages. The information required to carry out the comparison can be obtained from the web sites of the relevant Anti-Virus software suppliers.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 7

This session should be used to finish completing the log for this topic.

Section 2: Malicious Software (Malware)

Session 8

Candidates should work their way through the following online material and quizzes.

- Introduction
- Spyware
- Drive-By-Downloads
- Dealing with Spyware
- Spyware Clues
- Spyware Quiz1
- Spyware SQA2

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Spyware
- Dealing with Spyware

Session 9

Candidates should work their way through the following online material and quizzes. The importance of installing Anti-Spyware software should be noted.

- How Anti Spyware Software Works
- Adware
- Adware – Read the Small Print
- Dealing with Adware
- Adware Quiz

The Session should end with a brief review of the relevant points, eg:

- Anti/Spyware Software
- Characteristics of Adware
- Dealing with Adware

Session 10

Candidates should work their way through the following online material and quizzes. The dangers posed by Rogue Diallers to users of DialUp connections should be noted.

- Key Loggers
- Rogue Diallers
- DOS Attack
- Internet Threats Quiz

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Key Loggers
- Characteristics of Rogue Diallers
- Characteristics of DOS Attacks

Session 11

Candidates should work their way through the following online material and quizzes. The importance of Spam Filters and Anti-Spam Software should be noted.

- Spam
- How Spammers Work

- Spam Filters
- Anti Spam Software
- Spam Quiz 1
- Spam Quiz 2

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Spam
- Spam Filters and Anti-Spam Software

Session 12

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Malware
- Completion of log

Depending on the facilities available locally, the activities recorded in the log should be either:

3. Details of the installation of anti-spam and anti-spyware by the student. If local restrictions prevent the installation of relevant packages, it may be possible to install packages on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
4. Comparison of the features offered by three different anti-spam packages and three different anti-spyware packages. The information required to carry out the comparisons can be obtained from the web sites of the relevant software suppliers.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 13

This session should be used to finish completing the log for this topic.

Section 3: Other Internet Threats

Session 14

Candidates should work their way through the following online material and quizzes. They should know that genuine financial institutions will never ask for personal details to be submitted by email.

- Phishing
- Phishing Scam
- How to Defend Against Phishing
- Phishing Quiz

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Phishing
- Defences Against Phishing

Session 15

Candidates should work their way through the following online material and quizzes.

- Identity Theft
- Identity Theft Quiz
- Hoaxes
- Virus Hoaxes
- Hoax Activity
- Hoax Quiz

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Identity Theft
- Characteristics of Hoaxes

Session 16

Candidates should work their way through the following online material and quizzes.

- Ransomware
- Ransomware Quiz
- Hackers
- Hacker Activity
- Internet Threats Quiz 2

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Ransomware
- Characteristics of Hacking

Session 17

Candidates should work their way through the following online material and quizzes. They should be aware that any suspected instances of Cyberbullying or Grooming should always be reported to a responsible adult.

- Cyberbullying
- Tackling Cyberbullying
- Internet Grooming
- How to Protect Yourself
- Internet Threats Quiz 3

Grooming is a very sensitive topic, so the online materials in this area have been deliberately kept very low key. For those who wish to go into greater depth, useful material can be found at:

<http://www.uclan.ac.uk/host/cru/docs/NewCyberStalking.pdf#search=%22lancashire%20grooming%22>

The Session should end with a brief review of the relevant points, eg:

- Characteristics of Cyberbullying
- Characteristics of Grooming
- Protection against Cyberbullying and Grooming

Session 18

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Other Internet Threats
- Completion of Log

The log should give details of the steps taken by the student to protect himself / herself against Internet threats such as Phishing, Identity Theft, Hackers, Cyberbullying and Grooming.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Section 4: Internet Defences

Session 19

Candidates should work their way through the following online material and quizzes.

- Introduction
- Internet Defence Activity
- Avoiding Threats
- Removing Threats
- Internet Security Suites

The Session should end with a brief review of the relevant points, eg:

- Internet Defence Activity
- Avoiding and Removing Threats
- Internet Security Suites

Session 20

Candidates should work their way through the following online material and quizzes. They should recognise the importance of using strong passwords and keeping passwords secret.

- Passwords
- Password Security
- Password Security Activity
- Passwords Quiz 1
- Passwords Quiz 2

The Session should end with a brief review of the relevant points, eg:

- Passwords
- Password Security

Session 21

Candidates should work their way through the following online material and quizzes. They should be aware of the importance of using Firewalls and Content Filtering software on home machines, and backing up critical files regularly.

- Firewalls
- Firewall Quiz
- Proxy Servers
- Content Filtering
- Backup/Restore
- Internet Defences Quiz

The Session should end with a brief review of the relevant points, eg:

- Firewalls
- Proxy Servers
- Content Filtering
- Backup/Restore

Session 22

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Internet Defences Review
- Completion of Log

Depending on the facilities available locally, the activities recorded in the log should be either:

3. Details of the installation of firewall, content filtering and internet security software by the student. If local restrictions prevent the installation of relevant packages, it may be possible to install packages on a virtual machine by using **Microsoft Virtual PC** or **VMWare**.
4. Comparison of the features offered by two different firewall packages and two different content-filtering packages and two different internet security suites. The information required to carry out the comparisons can be obtained from the web sites of the relevant software suppliers.

The log should also give details of the steps taken by the student to generate secure passwords and backup and restore critical files. It should not contain examples of genuine passwords.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 23

This session should be used to finish completing the log for this topic.

Section 5: Legal Aspects

Session 24

Candidates should work their way through the following online material and quizzes. They should be aware of the dubious legality of P2P and the possibility of both P2P software and downloaded files introducing malicious software into a system.

- Downloading Files
- Why You Should Avoid P2P
- Alternatives to P2P

The Session should end with a brief review of the relevant points, eg:

- Dangers of P2P

Session 25

Candidates should work their way through the following online material. They should realize that the majority of information found on the Internet is likely to be copyright, and thus subject to restrictions on use.

- Copyright
- Copyright and the Internet
- Digital Rights Management

The Session should end with a brief review of the relevant points, eg:

- Copyright and the Internet
- Digital Rights Management

Session 26

Candidates should work their way through the following online material. They should realize the importance of ensuring that websites are accessible to users with disabilities.

- Disability Discrimination Legislation
- The Data Protection Act

The Session should end with a brief review of the relevant points, eg:

- Disability Discrimination Legislation
- The Data Protection Act

Session 27

Candidates should work their way through the following online material. They should be aware that the considerations regarding chat rooms apply equally to Instant Messaging and Social Networking sites.

- Chat Rooms

The Session should end with a brief review of the relevant points, eg:

- Chat Rooms

Session 28

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Review of Legal Aspects
- Completion of Log

The log should include details of the steps taken by the candidate to ensure that his/her own activities comply with all relevant legal requirements and safety recommendations, eg: detail of legal downloads made, steps taken to make websites accessible, steps taken to minimise display of personal information, etc.

The log must be in electronic form and capable of online submission. The recommended way of doing this is by means of a blog.

Session 29

This Session does not make use of the online materials. Instead, it should concentrate on the following areas:

- Course Review
- Final Completion of Logs

Any logs which need further attention should be completed at this stage, or arrangements made for their completion at some subsequent date.

Session 30

This session should be used to allow candidates to undertake the Online Assessment (MCQs). Arrangements should be made to allow candidates who do not complete this successfully to resit at a later date after appropriate remediation.

7. DELIVERY ISSUES

Teaching and Learning Materials

Online

An online version of the teaching and learning materials is available at <http://www.sqasolar.org.uk>

Moodle

A version of the materials hosted in SQAs Moodle VLE (Virtual Learning Environment) is available at <http://www.myqualifications.com>

Mobile

SQA have also produced a version of the Teaching and Learning materials that is ideal for those accessing them from a mobile phone or similar device with a small screen. This version can be accessed at <http://e-learning-computing.com/mobile>.

Assessment

Authentication

The amount of authentication will depend on the extent of control imposed on candidates during the assessment activities. For example, if candidates are closely supervised during most of the activities then there is no requirement for any authentication; if candidates are part-supervised during the activities (maybe as a result of large class size) then limited authentication is required; and if the candidate carries out many tasks unsupervised then authentication will have to be more rigorous.

Authentication should take the form of oral questioning of the candidate. The questions would relate to the candidate's experiences during the unit (those that relate to Outcome 4).

Appropriate questions would include:

- Tell me about your entry on viruses that you posted on 3 November.
- Your blog states that you watched a video about identity theft on 4 May. Did you enjoy it? What did you learn from it?
- What threats to system security did you come across during the unit?

Authentication is about giving confidence that the evidence belongs to the candidate. It is not an assessment of candidates' communication skills – especially their oral skills – so do not judge candidates on this basis. Nor is it a re-assessment of their knowledge of Internet safety. There is no requirement for candidates to answer every question correctly. The key question for assessors is: did the candidate satisfy you that the blog is an accurate record of their actual activities?

Re-assessment

Candidates who do not complete the short test successfully at the first attempt should be given a further opportunity to attempt it after appropriate remediation. The number of attempts allowed should be determined by the centre. A different test should be used for each attempt, however, the online version automatically generates a different test on each assessment occasion.

Formative assessment

Formative assessment gives candidates the opportunity to assess their learning before proceeding to summative assessment. The online learning materials include a number of short quizzes which are ideal for this purpose and should be attempted as candidates work

their way through the unit. Centres using the online testing system (SOLAR) for formative assessment, as a different test is generated automatically on each assessment occasion.

Online assessment

The knowledge assessment can easily be assessed online through SQA's e-assessment engine, called SOLAR. Solar can be used for summative assessments and can be used by teachers and lecturers to create formative and practice assessments.

If you are a Scottish FE college you can currently access the knowledge assessment in Solar. If you are another SQA centre and would also like to use the online assessment through Solar, then please contact the Solar Team on solar@sqa.org.uk. Visit the Solar website (www.sqasolar.org.uk) to see when we are next holding training events in the use of Solar.

Selection of blogging software

Almost any blogging tool can be used to create a weblog for assessment purposes. Centres will probably find it easier to use a hosted service rather than install blogging software themselves. Information about a number of suitable services can be found at:

http://en.wikibooks.org/wiki/Weblogs#Weblog_providers