National Unit specification: general information

Unit title: Internet Safety (SCQF Level 4)

Unit code: H1F6 10

Superclass:	CB
Publication date:	May 2016
Source:	Scottish Qualifications Authority
Version:	03

Summary

This Unit is aimed at **beginners** who want to learn how to use the Internet safely and responsibly.

The purpose of this Unit is to introduce learners to the main threats to personal safety when they are using the Internet, and how best to protect themselves from these threats. It covers topics such as: cyber hygiene, data security, and individual rights and responsibilities. The threats covered include: cyberbullying, cyberstalking, identity theft, sextortion and malware (such as ransomware).

As well as learning about the main threats to personal safety, learners will also gain practical skills in protecting themselves from these threats by learning, for example, how to use firewalls, virus protection, backup software and generally maintaining high standards of personal cyber hygiene.

On completion of this Unit, learners will understand the risks of working online and be able to take precautions to safeguard themselves.

This free-standing Unit is suitable for a wide range of learners and is particularly appropriate for young people, parents and mature Internet users.

Outcomes

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

Recommended entry

Entry is at the discretion of the centre. No previous knowledge or experience of computers or the Internet is required. However, it would be advantageous if candidates possessed basic IT skills which could be evidenced by having achieved Unit H3LJ 09 *Computer Basics* (SCQF Level 3).

National Unit specification: general information (cont.)

Unit title: Internet Safety (SCQF Level 4)

Credit points and level

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

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

Core Skills

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

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

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

National Unit specification: statement of standards

Unit title: Internet Safety (SCQF Level 4)

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

Outcome 1

Describe the risks that exist when using the Internet.

Performance Criteria

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

Outcome 2

Safeguard self when working online.

Performance Criteria

(a) Take precautions to protect personal safety and personal privacy.
(b) Protect personal information online.
(c) Check the identity of other online users.
(d) Describe the forms and characteristics of cyberbullying.
(e) Explain when and how to report online safety issues.
(f) Identify where to get online help and information on e-safety.

Outcome 3

Maintain data security and system performance.

Performance Criteria

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

National Unit specification: statement of standards (cont.)

Unit title: Internet Safety (SCQF Level 4)

Outcome 4

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

Performance Criteria

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

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge, experience, and understanding of their candidates to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that candidates have achieved all Outcomes and Performance Criteria. Sampling may be used in certain circumstances (see below) where the sample is sufficiently random and robust to clearly infer competence in the complete domain.

The evidence for all Outcomes in this Unit may be written, oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). Particular consideration should be given to digital formats and the use of multimedia.

Given the level of this Unit, the amount of evidence, and corresponding time spent on assessment, should be minimised, but sufficient to satisfy the performance criteria. Whenever possible, evidence should be a naturally occurring by-product of teaching and learning. However, it must be produced by the candidate. Authentication must be used where this is uncertain.

Evidence is required for **two** types of competence: **evidence of cognitive competence** (knowledge and understanding) and **evidence of practical competence** (practical abilities).

The evidence of cognitive competence will relate to Outcome 1 (all performance criteria), Outcome 2 (performance criteria d, e and f) and Outcome 4 (performance criteria a and b). Evidence is required for all of these cognitive competences unless it is generated through testing, in which case sampling may be used.

Evidence of cognitive competence may be sampled, so long as the sample is unknown and unpredictable to the candidate, and large enough to infer competence across the whole domain. Where sampling is used to assess the candidate’s knowledge and understanding, an appropriate pass mark should be set.

The evidence of practical competence will relate to Outcome 2 (performance criteria a, b and c), Outcome 3 (all performance criteria) and Outcome 4 (performance criterion c), and may take any appropriate form. Evidence is required for all of these practical (psychomotor) competences. Sampling of practical competence is not permissible. It is sufficient to demonstrate these practical competences **once**. For example, if an observation checklist is used to record practical competence, it is sufficient to observe the candidate taking precautions to protect personal safety and personal privacy on one occasion (Outcome 1, Performance criterion a).

The evidence for Outcome 4, PC (c), may be judged by exception. Candidates may be presumed to adhere to guidelines and procedures unless they prove otherwise. Separate evidence is not required to satisfy this criterion.

Evidence of practical competence may be produced over an extended period of time; but where it is generated without supervision some means of authentication must be carried out. The Guide to Assessment provides advice on methods of authentication.

When judging the standard of the evidence, cognisance should be taken of the SCQF Level of this Unit. The most relevant Level descriptions relating to the evidence of cognitive competence for this Unit are:

- basic knowledge
- simple facts and ideas
- knowledge of basic terminology
- identification of consequences of action/inaction.

The most relevant Level descriptions relating to the evidence of practical competence for this Unit are:

- relate knowledge to practical contexts
- use a few skills to complete straightforward tasks
- prepare for familiar and routine tasks
- select and use, with guidance, appropriate tools.

The Guidelines on Approaches to Assessment (see the Support Notes section of this Specification) provide specific examples of instruments of assessment.

National Unit specification: support notes

Unit title: Internet Safety (SCQF Level 4)

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

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

Guidance on the content and context for this Unit

The overall aim of this Unit is to enable learners to work safely and responsibly online. The Unit will provide learners with information about the safety factors and legal considerations which need to be taken account of when using the Internet and give them practical experience of using these. Learners should be aware that, at the time of writing, there is no clearly defined law governing cyberbullying or sextortion; there are several different laws that may apply in England, Wales and Scotland. It is anticipated that the Unit will be delivered over an extended period of time, during which learners can be observed in their natural environment applying their knowledge of Internet safety. The Unit covers all of the skills outlined in the 'Internet Safety for IT Users' qualification produced by e-Skills '(now the Tech Partnership)', the Sector Skills Council for Business and IT.

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

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

Outcome 1

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

Performance criterion (a) relates to identifying risks to users' personal safety and personal privacy. Learners should be aware that threats to personal safety and privacy include abusive behaviour ('cyberbullying'), inappropriate behaviour, grooming, cyberstalking and sextortion (extortion involving sex-related digital photos). They should appreciate that despite taking place in the virtual (online) world, all of these activities have consequences that can manifest in the physical world. Learners should be aware that these threats can appear in a variety of different contexts, eg text messages, chat rooms, e-mail, social networking sites and instant messaging. They should also be aware of the need to minimise their 'digital footprint' by minimising the amount of personal information they reveal online. It is always a good idea to remember the golden rule of social media and online communications: do not post, share or tweet content you wouldn't be comfortable sharing with the entire world.

Performance criterion (b) relates to identifying risks to the security of personal data.
All online activities contain an element of risk, eg shopping, texting, e-mails, phone calls, use of social media sites and browser searches. Learners should be aware that risks to the security of personal data includes malicious programs (including viruses, worms, trojans, spyware, adware), hackers, phishing, social engineering (attempts to trick someone into believing they are a friend or acquaintance) and identity theft. Learners should be aware that social engineering tactics include, but are not limited to, shoulder surfing and eavesdropping and should be able to identify examples from all of these categories.

Performance criterion (c) relates to identifying risks to system performance and integrity.
Learners 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 and adware) and hackers, and should be able to identify examples of all of these categories. Learners should also be made aware of non-existent ('hoax') threats (such as virus hoaxes) and emerging threats (which include 'ransomware').

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

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

Outcome 2

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

Performance criterion (b) relates to protecting personal information online.
Learners should be aware that using mobile devices, smartphones and tablets, in public places could also present a risk to their online personal data. Learners should be aware of the need to restrict the amount of personal information they reveal online.

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

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

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

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

Outcome 3

This Outcome relates to maintaining data security and system performance.

Performance criterion (a) relates to taking appropriate precautions to maintain security of personal data. Learners should be aware that precautions for maintaining the security of personal data include firewalls, software for detecting and disabling malicious programs or malware (including viruses, worms, trojans, spyware and adware) and e-mail filtering software (spam filters). They should be able to describe the precautions which can be taken in all these categories, including the use of Internet security suite, which may cover more than one category of threat. If an Internet security suite is not used, a range of different software programs will have to be collected to provide the cover for each of the various threats. Cyber hygiene should be routinely undertaken (cyber hygiene is a means of appropriately protecting and maintaining IT systems and other mobile devices and implements cyber security best practices), eg knowing what's connected to and running on a network, implementing key security settings to help protect systems, regularly updating all apps, software, and operating systems. They should also be aware that while system performance and data security are separate topics, the precautions taken may end up addressing the same issues

Performance criterion (b) relates to taking appropriate precautions to maintain system performance and integrity. Learners must be aware that precautions for maintaining system performance and integrity include firewalls, software for detecting and disabling malicious programs or malware (including viruses, worms, trojans, spyware and adware) and e-mail filtering software (spam filters). They must be able to describe the precautions which can be taken in all these categories, including the use of Internet security suites, which may cover more than one category of threat. If an Internet security product is not used, a range of different software programs will have to be collected to provide the cover for each of the various threats. Cyber hygiene should be routinely undertaken (cyber hygiene is a means of appropriately protecting and maintaining IT systems and other mobile devices and implements cyber security best practices), eg knowing what's connected to and running on a network, implementing key security settings to help protect systems, regularly updating all apps, software, and operating systems.

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

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

Outcome 4

This Outcome is about adhering to legal requirements, guidelines and procedures that apply when working online.

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

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

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

Guidance on learning and teaching approaches for this Unit

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

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

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

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

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

The use of case studies is recommended.

Learners should be aware that Cyberbullying in itself is not a crime, and is not covered by a specific law in the UK. However, by committing an act of cyberbullying, a person may be committing a criminal offence under a number of different acts that may differ across borders. Scotland, England, Northern Ireland and Wales may use different Acts to secure prosecutions. At the time of writing, reforms to existing Acts are being debated and new/reformed Acts may become law by the end of 2016.

Cyberbullying and the Law – [anti-bullying alliance]
http://www.anti-bullyingalliance.org.uk/resources/cyberbullying/cyberbullying-and-the-law/

The Scottish Law Commissions Paper on Cyber-crime affecting personal safety, privacy and reputation including cyberbullying - Promoting Law Reform - 2015
http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf

Existing Acts that may be used to secure prosecutions include:

Scottish Acts covering child protection: A national approach to anti-bullying.
http://www.gov.scot/Publications/2010/11/12120420/14

National Guidance for Child Protection in Scotland -Scottish Government 2014.
http://www.legislation.gov.uk/asp/2005/9/contents

Sexual Offences (Scotland) Act 2009 http://www.legislation.gov.uk/asp/2009/9/contents

Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005
http://www.legislation.gov.uk/asp/2005/9/contents

England, Wales and Northern Ireland might use other laws such as those described by the following:

The Cyber Smile Foundations - List of UK acts covering cyberbullying
https://www.cybersmile.org/advice-help/category/cyberbullying-and-the-law

Anti-Cyberbullying Laws in the UK - (October 2014) NoBullying.com
http://nobullying.com/anti-cyber-bullying-legislative-matters-in-the-uk/

Sexual offences - CPS Guide http://www.cps.gov.uk/news/fact_sheets/sexual_offences/

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

Unit title: Internet Safety (SCQF Level 4)

Guidance on approaches to assessment for this Unit

The approach to assessment for this Unit could be traditional or online.

A traditional approach to assessment for this Unit could comprise two assessments:

1. **Test** for cognitive competence.
2. **Observation checklist** for practical competence.

The test could be a multiple-choice test, comprising 20 multiple-choice questions covering the knowledge and understanding of this Unit (see Evidence Requirements). The pass mark (assuming four options are used in each question) would be 12 out of 20. The questions would relate to basic knowledge and understanding, and most would involve factual recall.

The observation checklist would record candidates completing each practical activity on at least one occasion. The assessor would complete the checklist as-and-when s/he observes the candidates satisfying each relevant Performance criterion (see Evidence Requirements).

A more contemporary approach to assessment would involve the candidate maintaining a **web log (blog)** of their learning and practical activities during this Unit. The blog should record, on a day-by-day or week-by-week basis, the teaching and learning that take place. The posts would have to be adequate (individually or collectively) to satisfy every Performance criterion in this Unit.

In this scenario, it would be adequate for candidates to describe their practical activities. For example, candidates could describe the precautions that they took to protect their personal safety and privacy (Outcome 2, Performance criterion a), rather than being observed actually doing it. However, the posts should provide enough detail to give the assessor confidence that the candidate has actually carried out the task and satisfied the associated Performance criterion. It would not be acceptable to simply post: “Today I protected my personal safety and privacy”. In this scenario, authentication would be vital (such as oral questioning) to confirm that the blog post was actually undertaken by the candidate and not simply invented.

National Unit specification: support notes (cont.)

Unit title: Internet Safety (SCQF Level 4)

Opportunities for the use of e-assessment

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

Opportunities for developing Core Skills

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

Disabled candidates and/or those with additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering whether any reasonable adjustments may be required. Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**

History of changes to Unit

Version	Description of change	Date
03	Minor amendments to wording of Outcomes 3 and 4 to add clarity. Minor amendments to wording of the following Performance Criteria to add clarity: Outcome 1 - (a) Outcome 2 - (a), (c) and (d) Outcome 4 - (b) and (c) Minor amendments made to 'General information' and 'Statement of Standards' sections. Amendments made to 'Support Notes' to add more clarity and detail and bring Unit up to date.	07/04/2016
02	Core Skills Component Critical Thinking at SCQF level 4 embedded.	17/05/2012

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Business Development and Customer Support team, telephone 0303 333 0330.