# National Unit Specification

## General information

## Unit title: Internet Safety (SCQF level 4)

## Unit code: J5V4 44

| | |
|---|---|
| **Superclass:** | CB |
| **Publication date:** | April 2022 |
| **Source:** | Scottish Qualifications Authority |
| **Version:** | 01 |

## Unit purpose

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, online racism and discriminatory behaviour, 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 unit is suitable for a wide range of learners and is particularly appropriate for young people, parents and mature internet users.

## Outcomes

On successful completion of the unit the learner will be able to:

1 Describe the risks that exist when using the internet.
2 Safeguard self when working online.
3 Maintain data security and system performance.

## National Unit Specification: General information (continued)

## Unit title: Internet Safety (SCQF level 4)

## Credit points and level

1 National Unit credit at Scottish Credit and Qualifications Framework (SCQF) level 4:
(6 SCQF credit points at SCQF level 4)

## Recommended entry to the unit

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 learners possessed basic IT skills that could be evidenced by having achieved unit J5V3 43 Computer Basics (SCQF level 3).

## Core Skills

Achievement of this unit gives automatic certification of the following:

| | |
|---|---|
| Core Skill component | Accessing Information (SCQF level 4) |

There are also opportunities to develop aspects of Core Skills which are highlighted in the support notes for this unit specification.

## Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

## Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

# 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) Explain the importance of internet safety.
(b) Identify key risks to online personal safety and personal privacy.
(c) Identify methods of protecting privacy and safety online.
(d) Identify tools to protect personal information online.
(e) Identify key websites to educate oneself on internet safety and privacy.

## Outcome 2

Safeguard self when working online.

### Performance criteria

(a) Take precautions to protect online personal safety and personal privacy.
(b) Identify methods of creating a strong password.
(c) Identify software to protect online personal safety and privacy.
(d) Identify hardware to protect online personal safety and privacy.
(e) Explain where to get online help and information on e-safety.
(f) Explain how to communicate safety online.

## Outcome 3

Maintain data security and system performance.

### Performance criteria

(a) Define data security and system performance.
(b) Describe the importance of data security for online use.
(c) Identify key types of data security to protect oneself online.
(d) Explain factors that can affect system performance.
(e) Explain methods of maintaining system performance.
(f) Explain how to maintain data security on a social networking site.

## **Unit title:** Internet Safety (SCQF level 4)

### Evidence requirements for this unit

Assessors should use their professional judgement, subject knowledge, experience, and understanding of their learners 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 learners 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 learner. Authentication must be used where this is uncertain.

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

The evidence of cognitive competence will relate to outcome 1 (all performance criteria), outcome 2 (performance criteria (e) and (f)) and outcome 3 (all performance criteria). Evidence is required for all 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 learner, and large enough to infer competence across the whole domain. Where sampling is used to assess the learner'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), (c) and (d)) and may take any appropriate form. Evidence is required for all 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 learner taking precautions to protect personal safety and personal privacy on one occasion (outcome 2, Performance Criterion (a)).

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.

## National Unit Specification: Statement of standards (continued)

## Unit title: Internet Safety (SCQF level 4)

When judging the standard of the evidence, cognisance should be taken of the SCQF level of this unit. The most relevant level descriptors 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 descriptors 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 guidance on approaches to assessment of this unit (see National Unit Support Notes section) provide specific examples of instruments of assessment.

## National Unit Support Notes

## Unit title: Internet Safety (SCQF level 4)

Unit support notes are offered as guidance and 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 risks that need to be considered when using the internet and give them practical experience of using tools to manage privacy and safety risks. It is anticipated that the unit will be delivered over an extended period, during which learners can be observed in their natural environment applying their knowledge of internet safety.

The current context for this unit is one of concern about the safety of people using the internet for a variety of purposes including work, learning and connecting with friends and family. This environment is partly the result of media stories relating to (for example) the abuse of young people or the financial deception of 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.

### Outcome 1

This outcome relates to the risks that can exist when using the internet.

Performance criterion (a) relates to the importance of internet safety. The world wide web is now used for a range of purposes including shopping, payment services, internet banking and mobile banking. Based on the highly accessible nature of the internet, there has been an unfortunate rise in online fraud and scams which reinforces the importance of internet security. For performance criterion (b), key threats to personal safety and privacy include abusive behaviour (cyberbullying and racism), 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 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, for example text messages, chat rooms, e-mail, social networking sites and instant messaging.

For performance criterion (c), learners should acknowledge the various approaches to protect privacy and safety online. Assessors should emphasise the need to avoid accessing unsecured public Wi-Fi on devices. Learners should be aware of the importance of not entering compromising information, like financial information, on non-secure websites. In terms of performance criterion (d), assessors should provide a demonstration of various tools which can be used to protect personal information online, such as passwords and contact details of the user. Learners should be introduced to password managers and the benefits of using this tool. Password managers generate individual passwords for the sites you visit. Because passwords are securely stored, password managers make it easier to maintain secure, unique passwords. Learners do not need to have a detailed knowledge of password managers but should understand the purpose and benefit of using this tool to protect personal information. For the final performance criterion, learners should have time to research various websites and information sources regarding online safety and privacy. This could be a good opportunity to hold a class discussion on the most comprehensive information sources on the matter. Key websites to be aware of, at the time of writing, include saferinternet.org.uk, ico.org.uk, ncsc.gov.uk and cybersmile.org. These websites also offer numerous tips and recommendations to help users protect personal information and maintain personal safety online, especially on social networking sites and chatrooms.

### 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. For performance criterion (b), 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 a password that doesn’t include repeat numbers of letters, is at least six characters and includes symbols where possible.

For performance criterion (c), assessors should highlight the growing number of software applications that can be used to protect online safety and privacy. For example, internet anonymity can be used to prevent the storage of personal information for longer than the current request. Additionally, antivirus software should be stressed as a key preventative method against hacking. This software can keep hackers from remotely taking over a computer, accessing personal and financial information, and tracking locations. Many antivirus software providers are available and frequently update their protection software as a defence against the latest viruses. For performance criterion (d), learners should have a basic understanding of various hardware to protect online safety and privacy. Common examples such as secure computer data storage (for example, a password protected USB) should be highlighted to learners.

For the final performance criterion, learners should acknowledge the best approaches to communicating safely with friends, family and other users online. If the learner witnesses inappropriate or suspicious behaviour, such as bullying, posting offensive content or violating terms of use, the assessor should state the importance of reporting this to site moderators, who have the authority to enforce the rules and terms. Furthermore, younger learners should be aware of the risks of oversharing online, especially to people who they do not know personally, and on public platforms.

## Unit title: Internet Safety (SCQF level 4)

**Outcome 3**

This outcome relates to maintaining data security and system performance.

Performance criterion (a) looks for a definition of data security and system performance. At this level, learners are not required to have a detailed understanding of both terms. An acceptable answer could be 'Data security refers to the process of protecting data from unauthorised access', and a definition for system performance could be 'the efficiency, speed and reliability of accessing a certain system'. For performance criterion (b), the importance of data security should be stressed to learners, especially younger learners who are unaware of the risks and dangers posed by the internet. Data security is about keeping data safe. With a heavier reliance on computers, there are a number of potential threats to the storage of data. Data can get lost due to system failure, corrupted by a computer virus, deleted or altered by a hacker. A simple user error can result in an overwritten or deleted file.

For performance criterion (d), learners should be provided with an overview of the factors that impact on system performance. It is not necessary at this level to have an in depth understanding. Excessive heat is one of the major factors that affects the performance of the system. To reduce the heat effect, a fan is installed with the power supply or the room can be air conditioned. Additionally, multiple applications running on the computer can have a negative impact on system performance. Multi-tasking tends to slow down the performance of the computer because memory is used to support more than one application compared to when one application has all the memory to itself. This means that the more applications that are running the slower the computer will perform. Likewise, if less or one application is running the performance of the computer will be faster. For performance criterion (e), assessors should state the methods of maintaining and/or improving system performance. For instance, every computer has numerous files and programs on its hard drive that haven't been used in a while or are unnecessary. Disk Cleanup allows users to find which applications and files can be deleted from their computers, freeing up drive space. For the final performance criterion, learners should acknowledge the approaches that can be taken to maintain data security on social networking sites. Learners should be encouraged to manage the information shared with friends and acquaintances. If the learner is looking to create a public persona as a blogger or expert, an open profile or a 'fan' page can be used to encourage broad engagement. In contrast, a personal profile should be used to keep real friends and family (the ones known and trusted) up to date with daily life events.

## Guidance on approaches to delivery of 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 the support notes. While teaching will necessarily focus on a specific product, the generic features of the class of software should be emphasised.

An important outcome of this unit is that learners develop an appropriate technical vocabulary. Terminology and underpinning knowledge should be introduced in a practical context.

## National Unit Support Notes (continued)

## Unit title: Internet Safety (SCQF level 4)

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 three outcomes.

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 gaming community sites, or online travel blogs.

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.

## Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

It is possible to deliver and assess this unit remotely via video conferencing platforms.

A range of assessment approaches may be taken to assess each performance criterion within each outcome. Examples of assessment approaches could include written reports, recorded videos and the development of a weblog. In the case that the learner wishes to use a weblog to collate evidence, this should record, on a day-by-day or week-by-week basis, the teaching and learning that takes place. The posts should be adequate (individually or collectively) to satisfy every performance criterion in this unit specification. For example, learners could describe the precautions that they took to protect their personal safety and privacy (outcome 2, performance criterion (a), rather than being observed doing it.

It is important to note that assessments should be taken under controlled conditions to ensure the authenticity of the learner evidence. If evidence is generated without supervision (for example, remotely), assessors can use oral questioning to ensure that learner evidence is genuine.

## National Unit Support Notes (continued)

## Unit title: Internet Safety (SCQF level 4)

## Opportunities for 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 learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

## Opportunities for developing Core and other essential skills

The Core Skill component of Information and Communication Technology: Accessing Information is embedded in this unit at SQCF level 4. Learners will also have opportunities to develop the Critical Thinking component of the Problem Solving Core Skill.

## History of changes to unit

| Version | Description of change | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

© Scottish Qualifications Authority 2022

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

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

## General information for learners

## **Unit title:** Internet Safety (SCQF level 4)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit will help you develop basic knowledge of internet safety and the methods of maintaining online privacy and security. A key goal of this unit is to provide with you with guidance on creating a strong password, identifying tools to protect personal information online as well as communicating safely on digital platforms such as chatrooms and social networking sites.

The key skills that you will learn in this unit include:

- The methods of protecting online personal safety and privacy.
- Identifying software to protect online personal safety and privacy.
- Defining data security and system performance.
- Describing the importance of data security for online use.
- Identifying key types of data security to protect oneself online.
- Explaining factors which can affect system performance.
- Explaining methods of maintaining system performance.
- Explaining how to maintain data security on a social networking site.

The unit can be used for personal or business purposes. You could use your knowledge and skills to help you communicate safely with friends and family members online or understand how you can improve system performance when starting an online business.

The assessment of this unit may take different forms and may be delivered in a remote learning environment using video conferencing tools. However, it is important that your assessor ensures the authenticity of your evidence through oral questioning or by asking you to complete an authenticity statement.

The unit is for beginners. No previous knowledge or digital skills are required.

On successful completion of this unit you will automatically achieve the Core Skill component of Accessing Information in Information and Communication Technology at SCQF level 4 and you could progress to other qualifications including National Progression Awards in Cyber Security (SCQF levels 4, 5 and 6).