National Unit Specification

General information

Unit title: Network Literacy (SCQF level 4)

Unit code: J6B7 44

Superclass:	CB
Publication date:	May 2022
Source:	Scottish Qualifications Authority
Version:	02 (September 2022)

Unit purpose

This is a non-specialist unit for those who wish to acquire knowledge and skills in using networks in a non-technical environment, such as in the home and on the move. It aims to educate citizens in the productive, safe, and responsible use of current network technologies. This unit focuses on the fundamentals of networks including what they are, how they are used and how learners can safely set up a basic network.

This unit is suitable for all learners and no previous knowledge or experience of networks or computing is required. The unit introduces the basic concepts of networks and where they are used both personally and in society. It will enable learners to gain a familiarity with the social and environmental impact of networks, network terminology, basic security measures required and practical experience in establishing a basic network.

On completion of this unit, learners will possess a basic understanding of digital networking and be able to apply this to personal networks at home and the 'Internet of Things'. Learners may wish to take this unit alongside units Information Literacy (SCQF level 4) and Social Media Literacy (SCQF level 4) as part of the National Progression Award Digital Literacies (SCQF level 4) or progress to more advanced units such as Network Literacy (SCQF level 5) to further develop their knowledge and skills.

Outcomes

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

1   Define the impact of networks in society.
2   Define network safety and security processes.
3   Set up a simple network.

National Unit Specification: General information (continued)

Unit title: Network Literacy (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 experience is required.

Core Skills

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

Core Skill component   Accessing Information 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.

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.

This unit may be offered stand-alone or as part of the National Progression Award in Digital Literacies at SCQF level 4. If offered as part of the group award there may be opportunities to combine and integrate teaching and learning across units. There may also be the opportunities to combine evidence requirements and integrate assessments.

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: Network Literacy (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

Define the impact of networks in society.

Performance criteria

(a) List different types of networks.
(b) List types of internet services.
(c) List network services.
(d) List hardware and software components in a network.
(e) Use correct networking terminology.
(f) Explain the environmental impact of networks.

Outcome 2

Define network safety and security processes.

Performance criteria

(a) List the main safety and security issues relating to networks.
(b) List methods of maintaining safety and security on different networks.
(c) Explain the importance of online safety and personal security in networking.
(d) Explain cyber security threats that could impact personal security.
(e) Explain the importance of keeping data secure in networks.

Outcome 3

Set up a simple network.

Performance criteria

(a) Connect to a range of networks using hardware and software.
(b) Identify common errors when connecting to a network.
(c) Resolve basic network connectivity errors.
(d) Connect to a network following online safety and security protocols.

National Unit Specification: Statement of standards (continued)

Unit title: Network Literacy (SCQF level 4)

Evidence requirements for this unit

Assessors should use their professional judgement, subject knowledge, and 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. Assessors can best achieve this by concentrating on the most common and current technologies in use today.

Evidence is required to demonstrate that learners have achieved all outcomes and performance criteria. However, sampling may be used in certain circumstances where the sample is sufficiently random and robust to clearly infer competence in the full domain.

The evidence for this unit may be written or 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). Consideration should be given to digital formats and the use of multimedia. It is recommended that evidence is collected for the unit as a whole and is a naturally occurring by-product of teaching and learning. Holistic assessment (within and across outcomes) is encouraged where possible.

Evidence must span a range of device types and network usage. To facilitate this, learners will carry out a range of practical activities using commonly encountered devices and network services. The hardware and software to be used is discretionary but must be current.

Evidence is required for two types of competence: evidence of cognitive competence (knowledge and understanding) and evidence of practical competence (practical abilities). In certain circumstances, the evidence of cognitive competence may be sampled; the sample must be sufficiently random and robust. For example, if a traditional test is used to assess learners' knowledge and understanding, this test may sample across the knowledge domain; however, if a portfolio approach is taken then it would not be appropriate to sample, and evidence of **every** cognitive competence would be required. Evidence of practical competence cannot be sampled; however, the amount of evidence is left to the professional judgement of the assessor and should be the minimum compatible with the requirements of this unit. Evidence of practical competence should be produced over an extended period and in open-book conditions, for example through completion of a manual or digital logbook, video diary or e-portfolio. Learners should have access to help files and notes as well as appropriate online resources.

Evidence must be produced under controlled conditions. However, the amount of control will vary from context to context. For example, evidence of cognitive competence could take the form of a test, which would permit highly controlled conditions (which would include closed book assessment). Alternatively, evidence could be generated using a web log, written over an extended period at varying locations, which would not permit such close control. In every case, assessment must be controlled to some extent. Where the amount of control is low, the amount of authentication should rise. It is not acceptable to produce evidence in lightly controlled conditions with little authentication.

National Unit Specification: Statement of standards (continued)

Unit title: Network Literacy (SCQF level 4)

Authentication may take various forms including, but not limited to, oral questioning and plagiarism checks. Some forms of evidence generation (such as video recordings) have intrinsic authentication and would require no further means of verification. Where evidence is not generated under closely controlled conditions (for example, out of class) then a statement of authenticity should be provided by the learner to verify the work as their own and state any necessary sources and permissions. The *Guide to Assessment* provides further advice on methods of authentication.

Evidence for this unit should be generated naturally, as a by-product of teaching and learning, and integrated into as few assessment tasks as possible. The Guidance on approaches to assessment of this unit in the National Unit support notes section of this specification provides specific examples of instruments of assessment that seek to do this.

National Unit Support Notes

Unit title: Network Literacy (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 general context for this unit is the 'Internet of Things' (IoT), the idea that a wide range of devices are now connected to the internet. Learners may have varying degrees of experience and dependence on the IoT, and the scale of currency may be dependent on factors such as the age of the learner. This unit will deliver concepts of the internet as a network of networks that plays a fundamental role in society, the importance of safety and security when using networks and practical experience in setting up a basic network.

The purpose of this unit is to deliver basic knowledge and skills in the use of network resources and devices. This unit is intended for non-specialists and should be delivered in that context.

Throughout the unit, the terminology used means specific things. The phrase 'network hardware' refers to the infrastructure components used in networking such as routers and switches, as well as the client devices such as computers and smartphones, etc used to connect. The phrase 'network software' refers to software used on these client devices to facilitate usage of the network services, for example, email clients or web browsers. Finally, 'network services' refers to the reason the network is being used, for example, email, web browsing, social media, etc. The development of learners' technical terminology is important. Learners should be introduced to the correct terminology and encouraged to use the technical terms throughout.

At this level (SCQF level 4) treatment of every topic should be basic. Teaching should focus on imparting key knowledge and skills.

Outcome 1: This outcome is designed to provide a basic introduction to the field of network literacy. Whilst the learner may have used applications dependent upon networks, they may not be aware of the role networks play.

A key aspect of this outcome is for learners to gain an understanding of the underpinning role networks play personally and in society. Learners should be encouraged to reflect on their personal usage of networked systems in as many forms as possible. For example, personal uses at home may include computers, gaming devices, smart watches, and security systems. Examples of societal uses may include satellite navigation, traffic control systems, school, or workplace networks and how these are connected. Terminology at this level should be basic with the concept of routers, local area networks (LANs), wide area networks (WANs), and cloud networking introduced with limited amount of technical detail. The Internet of Things (IoT) should be linked to current and developing trends.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

Performance criteria (a), (b), (c) and (d) should be high level and broad to give learners insight into the range and depth of personal and societal reliance on networks. It would be reasonable at this level to introduce the concept that networks impact global citizens and a general appreciation that networks play a major part in global politics and economics.

Performance criterion (a) enables learners to gain an understanding of the Internet of Things (IoT) and cloud storage as a network of networks, with a basic appreciation that these networks are served in several ways that are continually being improved and developed. The evolution of internet services from dial up, cable broadband, wireless broadband, satellite, and Li-Fi would help learners appreciate the rapid rate of change in services offered.

Understanding types of network connections available serve different purposes. For example, wireless broadband (Wi-Fi) is appropriate for mobile hardware as the network is available on the move whereas a dedicated leased line would be appropriate for a large organisation that requires greater network speed, volume, and privacy. An appreciation of 4G/5G, Wi-Fi and LAN would help build learners' terminology. with the focus on the practical benefits each brings rather than technical differences.

Performance criterion (b) provides learners with an appreciation of the wide range of devices that can be connected to the Internet of Things. Learners should gain an understanding that the IoT has evolved and continues to evolve at a fast pace, and that societies' dependency has grown with it

Performance criterion (c) should focus on identifying network services used in day-to-day life. Learners should be aware that use of social media platforms, e-sports, virtual meetings, and any other modern service that applies, is a networked service.

Performance criterion (d) enables learners to identify the difference between hardware and software and the basic components required for networking. Hardware examples include computers, tablets and laptops, smart watches, smart TVs, smartphones, and gaming devices. In addition, learners should also be able to identify the most common type of infrastructure hardware. An example of this at time of writing would be a router.

Through performance criterion (d) learners will also be able to identify end user software applications. It is likely that learners are already familiar with a wide range of software applications and brands of network services through their general usage but may not be aware that each application depends on different software. At this level, learners' understanding will be a basic list of software applications.

Use of correct terminology (performance criterion (e)) should be encouraged throughout the outcome. At this introductory level an understanding of broad terminology, rather than technical specifications, is expected.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

Performance criterion (f) provides the learner with a basic understanding of the environmental impact of networks. An objective overview of the pros and cons of the environmental impact is required. Whilst networks have a carbon footprint of their own, they also prevent carbon footprint being generated elsewhere. Basic examples would be the environmental impact of traditional postal mail against email or working from home rather than commuting. Cloud storage helps to balance network energy consumption and more efficient use of water resources. Learners should also be given the opportunity to explore ways they could reduce their network environmental impact such as deleting unwanted photos from cloud storage or avoiding the larger carbon footprint by not using 'reply to all' in email.

Outcome 2: This outcome is designed to provide learners with an awareness of the risks associated with network usage and basic concepts for keeping safe and secure whilst using networks.

Performance criteria (a) and (b) cover risks and methods to mitigate them while performance criteria (c), (d) and (e) give learners an understanding of how to protect themselves and data.

As performance criteria (a) and (b) are interlinked learners would benefit from threats and mitigations being correlated. Performance criterion (a) enables learners to gain a basic understanding of contemporary safety and security issues that can occur with network usage. At this level, learners will gain an understanding of identification tools such as passwords, biometric security, PIN codes and the importance of keeping these secure. This criterion also provides a basic introduction to cyber security and some of the most common styles of threat present. At the time of writing, examples include social engineering, denial of service, man-in-middle, backdoors, keyloggers, spam, general malware, and common scams such as spam text messages and emails.

Performance criterion (b) enables learners to gain a basic understanding of contemporary safety methods that can be used to mitigate the risks identified. At the time of writing, examples include firewalls, anti-virus software, user training, anti-malware, secure passwords, digital certificates, social media settings and Wi-Fi security.

Performance criterion (c) enables learners to expand on the knowledge gained through Performance criteria (a) and (b) and should give them a basic insight into the risks being online poses and how to protect themselves when using networked devices. Learners should be able to review their personal settings on any networks they are connected to, find, and set the most appropriate privacy settings. Learners should also be encouraged to review the most up to date practices using the online safety guidelines available from network service suppliers. Learners should be advised how to recognise spam and unsolicited texts and emails. referencing the many scams, how these arise and how to deal with them.

Learners should also gain non-technical skills in maintaining their online safety by recognising that threats from online grooming, cyber bullying and social engineering exist. Learners should understand the implications of sharing information on networks that could make them vulnerable to such threats. For example, posting on social media that you are going on holiday could make your home at risk of burglary. It would also benefit learners if they were made aware of the mental health issues that can arise from over or misuse of online platforms, current organisations that offer help for individuals and how to report instances of online abuse.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

Performance criterion (d) enables learners to expand on the knowledge gained and should introduce them to contemporary cyber security threats and how they can be mitigated. At the time of writing, examples include firewalls, antivirus software and securing passwords.

Performance criterion (e) equips learners with knowledge of the value of data, the importance of keeping their data secure and actions to take if they find their data has been breached. Where performance criterion (a) has introduced learners to the types of data breaches that can occur, this criterion expands understanding of how they can keep their data safe. The principles of the Data Protection Act and GDPR for individuals and organisations should be introduced to highlight that all data has a value. Different types of data that should be protected would include 'direct' data, that is passwords, bank details, national insurance numbers, telephone numbers, and 'indirect' data, that is a pet's name posted on social media, birthday celebrations, reverse photos, etc. A balanced view should be portrayed, not judging *what* personal data is being shared but *how* data, if not stored securely, can be taken, or stolen from network services and used for other purposes in a variety of different ways. Learners should be made aware that storing with secure passwords on trusted networked services, using appropriate content sharing and network settings can reduce the likelihood of data being breached.

Learners would also benefit from knowing what to do if they find their data has been breached. For example, network services have complaints departments that can be contacted and asked to remove data if held outwith the principles of both the Data Protection Act and GDPR guidelines.

Outcome 3: This outcome is designed to give learners practical experience in setting up a simple network.

Performance criterion (a) builds on the introduction received in outcome 1 performance criterion (d) to a range of hardware devices and software applications. A variety of the most common hardware devices should be demonstrated, for example a smart phone, laptop, and smart watch. Where possible, learners would further benefit from using their own hardware (phone or tablet), as this would make the skills gained more practical. A variety of appropriate software packages would best demonstrate variation in setting up a network connection and provide learners with experience in answering the different questions required. Practical implementation of password control and security should be covered as part of this criterion and overlaps with performance criterion (d). Devices used should be connected using a router or current equivalent using an IP address and using Wi-Fi or the most common technique available to give learners experience in selecting the most effective connection type. Learners will gain an understanding that each router has a different IP address and how to locate it on the router.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

Performance criterion (b) allows learners to gain practical experience in identifying basic common errors that occur when connecting to a network. This feeds directly into Performance criterion (c) so a holistic approach to both criteria is encouraged. At this level learners will gain a basic understanding that there are many types of network errors, and the errors can be with the hardware, software, network, or human. Hardware, for example, may be out of memory, software applications may need a version update, the router may have low signal quality, or the IP address may have been entered incorrectly. Learners should also understand how to check for network outages using real time monitoring search engines and the internet for guidance on error messages received. At this level learners would be expected to identify where the error within the network set up occurred.

Performance criterion (c) allows learners to gain practical experience in resolving basic errors. These may have occurred naturally through performance criteria (a) and (b). The practical resolution could cover checking memory on the device and clearing out if required, checking software version used and updating if needed, checking the router's signal strength, and resetting or rebooting, reinputting the IP address or password. If the error is down to a network outage learners should understand that this is outwith their control, that guidance received from the internet should be checked for accuracy and only used if the source is reliable.

Performance criterion (d) allows learners to apply practical online safety protocols when connecting to networks. From outcome 2 performance criteria (a) and (d), learners will have gained a basic understanding of the threats and mitigations that exist online. This performance criterion has more emphasis on the technical mitigations covered rather than social engineering. At the time of writing examples of contemporary mitigations suitable for this level include checking firewalls in place, anti-virus software is up to date, anti-malware is in place, passwords are secure, social media settings are set appropriately and Wi-Fi is secure. Learners should also be aware that Wi-Fi security is particularly vulnerable when using an unsecured network, for example in a café.

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. Outcome 3 is designed to complement the teaching of outcomes 1 and 2 with practical skills. Teaching should be delivered so that learners will gain transferable skills and should not overly focus on a single network device or network system.

To facilitate the practical parts of the unit, learners will require access to various wireless client devices and different portable devices. Access to a wireless router or access point will also be necessary. If permitted, existing wireless infrastructure could be used since no configuration of these devices will be necessary. Network software may also be useful.

Learners will also require access to the internet to access various services. This does not need to involve any wireless connectivity.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

At this level, it is expected that learning will be a mix of assessor-led and self- or peer-learning. New concepts should be introduced by the assessor. Self- or peer-learning should be carefully devised and monitored. Opportunities should be taken to motivate learners using engaging technology such as multimedia (for example, music and video), social media (social networks and blogs) and computer games, and competences delivered in that context (for example, through online music services, such as Spotify™, that permit network sharing and collaboration).

The distribution of time over the three outcomes is at the discretion of the centre and thus will be influenced by several factors such as the actual technologies utilised. However, to emphasise the need for a 'learn by doing' approach, a possible distribution is as follows:

♦   Outcome 1: 8 hours.
♦   Outcome 2: 8 hours.
♦   Outcome 3: 24 hours.

Throughout this unit activities should relate to the personal or vocational interests of learners, and they should be encouraged to become confident with as wide a range of network services as possible. There are many online resources available to aid teaching and learning, with the unit outcomes well served by videos and podcasts, and case studies used to relate concepts to real life situations. Learners should be given opportunities to form discussion groups, facilitated by the tutor, for example to explore topics such as personal online privacy and safety issues and cyber security threats and mitigations.

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.

A traditional approach to assessment would involve the testing of knowledge through a closed book selected response test spanning outcomes 1 and 2. It is recommended that if this approach is adopted then all the knowledge and understanding from outcomes 1 and 2 are combined into a single test that samples from the knowledge domain, with an appropriate pass mark. A separate open-book practical assessment would be used to cover the required performance criteria for outcome 3.

Outcome 3 could be assessed through observation of learner activity throughout the duration of the unit and recorded on a checklist, or by learners completing a logbook containing appropriate screenshots, photographs, or other digital artefacts as evidence. Learners could be presented with a themed 'case study' style activity with the opportunity to demonstrate performance through a project, perhaps a realistic home or business networking scenario. In an open-book approach learners may have access to supporting materials such as notes, textbooks, summaries, and other resources.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

Another approach to assessment would be for learners to create and maintain a web log. This would record, on a daily or weekly basis, what learners learn and what they do with each post satisfying the related performance criteria. So, for example, the post that relates to outcome 1, performance criterion (a), would have to list enough network items.

When practical activity is recorded on a blog, authentication could involve a photograph or video of learning activity or a screenshot illustrating the criterion (such as a screen shot of a successful network service connection). Not every practical task would require authentication; at this level it is acceptable for some posts to be a simple description of appropriate practical activities. When necessary, separate authentication (such as oral questioning) could be used for verification purposes. The critical aspect is that the blog is an overall accurate reflection of the practical activities (and, therefore, the associated skills) obtained out by the learner during completion of the unit.

Another approach would involve the creation and maintenance of an e-portfolio. If the e-portfolio was created by the learner on a network service, this could satisfy outcome 3 (a). The e-portfolio would include all the descriptions and explanations necessary to satisfy the criteria relating to cognitive competencies (in this case, there is no justification for sampling), together with digital artefacts that provide evidence of their practical abilities. The latter [digital artefacts] would include screenshots, digital images, digital audio, and video recordings, etc. that collectively evidence the learner's' practical competencies. Some form of authentication would be required for a significant proportion of the gathered items, but this could be as simple as a statement of originality, signed by the learner, and counter-signed by the assessor, or a digital audio recording of a brief question-and-answer session between the learner and the assessor.

When necessary, separate authentication (such as oral questioning) could be used for verification purposes. The critical aspect is that the work produced is an overall accurate reflection of the required practical activities (and, therefore, the associated skills) obtained by the learner during completion of the unit. A checklist could be used to verify that learners have achieved the required knowledge and skills as set out in the performance criteria.

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 that 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**.

National Unit Support Notes (continued)

Unit title: Network Literacy (SCQF level 4)

Opportunities for developing Core and other essential skills

The Accessing Information component of Information and Communication Technology at SCQF level 4 is embedded in this unit. When a learner achieves the unit, their Core Skills profile will also be updated to include this component.

This unit provides opportunity to deliver aspects of the following Core Skills at SCQF level 4:

♦ Information and Communication Technology (ICT).
♦ Problem Solving.

Learners will undertake a range of tasks to enable them to develop these aspects such as:

♦ the selection and start-up of software (when using networks),
♦ use help facilities,
♦ enter and edit data (when using networks for social or learning purposes).

In addition to Core Skills, this unit provides opportunities for leaners to develop digital citizenship and employability skills and improve digital literacy due to the variety of software that they may use.

History of changes to unit

Version	Description of change	Date
02	Core Skills Component Accessing Information at SCQF level 4 embedded.	06/09/22

General information for learners

Unit title: Network Literacy (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 aims to educate you in the importance, responsible and secure use of modern networks in a variety of common ways. It is not necessary to have any prior knowledge of networks. It covers basic but important knowledge about networking and the skills needed to use networks securely and responsibly in everyday life.

Studying the unit will help you understand a variety of network devices and how they connect to the Internet of Things. You will develop skills in safely setting up personal network tools and actions to take if your safety is compromised. You will learn about the potential impact of computer networks on the environment and simple steps to reduce your network carbon footprint. You will develop a range of basic skills and competences to use networks personally on a daily basis.

The unit covers a wide range of knowledge and skills including:

♦   The need to use a network correctly and responsibly.
♦   The types of hardware and software used in networks.
♦   The range of common services provided by networks in common use today.
♦   The need to ensure networks are secure and the consequences of not doing so.
♦   Basic common threats that networks and users face and how they can be mitigated.
♦   Basic awareness of the environmental impact of networks.
♦   How to connect safely to a wireless network.
♦   How to access network services settings.
♦   Practical steps to reduce your network carbon footprint.

This unit is designed for learners with no previous experience of computing. It is particularly suitable for those who want to learn the basics of networks and available services, and how to keep safe whilst doing so to allow online participation in modern society.

To pass the unit, you will be asked to complete an assessment. This might include taking a multiple-choice test, creating a blog, or completing a project style activity where you demonstrate the knowledge and skills you have learned. Your assessor will provide more information on how you will be assessed.

A key goal of this unit is to enable you to become a knowledgeable, responsible, and active user of digital technologies and networks so that you can confidently use them for personal purposes.

On completion of this unit, you will be able to use smartphones, tablets, PCs, and other digital devices for a wide range of personal and social purposes, including accessing and using a variety of internet services.

This unit will also provide you with the opportunity to develop aspects of the Core Skills of Information and Communication Technology (ICT) and Problem Solving at SCQF level 4 and enhance your digital literacy skills.

General information for learners (continued)

Unit title: Network Literacy (SCQF level 4)

This unit is part of a series of units on network literacy. You may progress to the next unit in the series (Network Literacy at SCQF level 5) on completion of this unit if you wish to improve your knowledge and skills in this area.

The Accessing Information component of Information and Communication Technology at SCQF level 4 is embedded in this unit. When you achieve the unit, your Core Skills profile will also be updated to include this component.