National Unit specification

General information

Unit title: Data Security (SCQF level 4)

Unit code: H9E2 44

Superclass: CC

Publication date: July 2015

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this Unit is to provide an introduction to the use of personal data and data security, the risks associated with storing and sharing personal data, and to provide experience of basic data protection.

The Unit provides a broad overview of what personal data is, how it is measured, where it is held, and how it is used and shared in an interconnected digital world.

A specific aim of the Unit is to raise awareness of the risks associated with storing and sharing personal data, and simple strategies to protect data.

On completion of this Unit, learners will have the basic knowledge and skills in data security, and be able to demonstrate basic practical methods of protecting personal data. Learners may progress to the *Data Security* Unit at SCQF level 5 or similar National Units.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF level 4.

Outcomes

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

1 Describe how personal data can be stored, used and shared by social media.
2 Identify the risks associated with storing and sharing personal data.
3 Apply basic practical methods of protecting personal data.

National Unit specification: General information (cont)

Unit title: Data Security (SCQF level 4)

Credit points and level

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

Recommended entry to the Unit

No prior knowledge, skills or experience in the field of Data Security is expected of learners prior to undertaking this Unit.

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the Support Notes for this Unit specification.

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

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.

The Assessment Support Pack (ASP) for this Unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

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: **Data** Security (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 how personal data can be stored, used and shared by social media.

Performance Criteria

(a) Describe what data is.
(b) Describe how and where data is stored.
(c) State the main ways personal data is used online.
(d) Describe how companies share personal data.

Outcome 2

Identify the risks associated with storing and sharing personal data.

Performance Criteria

(a) Identify the main sources of risks to online data.
(b) Identify the general principles of keeping personal data secure online.
(c) Identify what types of personal data should and should not be shared online.
(d) Identify real life examples of the negative impact of data sharing.

Outcome 3

Apply basic practical methods of protecting personal data.

Performance Criteria

(a) Select strong passwords to keep data secure.
(b) Check the security of websites before entering personal data.
(c) Protect personal data in social media services.

National Unit specification: Statement of standards (cont)

Unit title: Data Security (SCQF level 4)

Evidence Requirements for this Unit

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. However, sampling may be used in certain circumstances (see below).

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). 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: 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 (all Performance Criteria).

The evidence of cognitive competence may be sampled across the knowledge domain defined by this Unit specification, so long as the sample is unknown, and unpredictable, to the learner. 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 3 (all Performance Criteria) and can take any appropriate form. However, it should be produced with an emphasis on how individuals can take basic steps to improve security around personal data they store online. Candidates must apply basic practical methods of protecting personal data on at least **one** occasion.

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.

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

National Unit Support Notes

Unit title: Data Security (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

Throughout this Unit it is important to present both the positive and negative implications of storing personal data online. Understanding whether it is appropriate to share particular types of data is key, and consideration should be given to real life examples where sharing personal data has had negative consequences.

Throughout this Unit learners must adhere to basic ethical standards of practice.

Outcome 1

This Outcome introduces the concept of data, and what data is. It is possible that learners may have little awareness of the concept of data, and what personal data entails. Understanding that the information they share about themselves online is classed as 'personal data' is an important first step.

This foundation can be built on and expanded by investigating where data is stored online. Learners will likely be able to relate this storage of data with examples from their own online usage, such as use of social media, email accounts and visiting websites.

Understanding where data is stored can be expanded to include how personal data is used online. This falls into three main categories;

(a) How personal data is used by you.
(b) How personal data is used by other people.
(c) How personal data is used by companies.

Topics such as the buying/selling of personal data can be covered here, and the use of personal data to target advertising at individuals based on their circumstances/preferences could also be covered.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 4)

Outcome 2

This Outcome builds on the foundation of what personal data is and how it can be used, highlighting the risks which are associated with using and storing personal data online.

Learners should be encouraged to question why there could be risks with having their personal data stored online, and to think about what sorts of data should and should not be shared online. For example, sharing too much personal information on social media (such as location or date of birth) could put someone at risk of identity theft, or not being careful about where you enter bank details or passwords could also cause a security risk.

The specific risks posed by computer networks should be emphasised since their connectivity presents particular risks to personal data. At this level, learners' understanding of these risks need not be technical (such as understanding the TCP/IP protocol).

Examples can be presented here of instances where personal data sharing has had negative consequences. For example, celebrities, politicians or businesspeople who have got into trouble in the media for posting information online. This could also include companies who have 'lost' or 'exposed' people's personal data.

Outcome 3

A range of general principles for keeping personal data secure online should be covered. This includes:

(a) Creating strong passwords, and changing passwords regularly:
  (i) what is a strong password?
  (ii) why do my passwords need to be strong?
  (iii) why should I change my passwords regularly?

(b) Checking that websites are secure before entering any personal information:
  (i) what the green padlock/https:// mean.
  (ii) how else to check a site is secure.
  (iii) using public/open networks.

(c) Checking privacy settings on social media and being aware of what information others:
  (i) can see about you.
  (ii) check who can see your personal information.
  (iii) limit what you share (age, location, DOB).
  (iv) think about who might see what you post.
  (v) make sure you log out after using a site (esp on public networks).
  (vi) don't connect with people you don't know.

National Unit Support Notes (cont)

Unit title: Data Security (SCQF level 4)

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 identifying personal data stored online, and are able to identify their own personal data, and how much of their data is currently visible online to others. Learners should adhere to appropriate safety and etiquette guidelines whilst carrying out these activities.

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.

Outcome 1 requires a basic level of knowledge of what data is and how it is stored. Evidence can be captured in various ways, such as written presentations, oral presentations, or the creation of a poster/short film/animation to demonstrate understanding of these concepts. A traditional test which appropriately samples knowledge is also acceptable.

Outcome 2 covers the risks of storing and sharing personal data, and general principles for keeping data secure. Evidence for this Unit can take a variety of forms; similar methods to Outcome 1 are acceptable.

Outcome 3 is focussed on practical methods of keeping personal data secure online. This could be in the form of an observation checklist completed and signed by the assessor after observing candidates carry out practical tasks. This could also be in the form of an ‘audit’ — on a friend or family member's personal online security. The candidate could interview a friend or family member, explain the risks of storing personal data online, and advise them on methods of improving their online security. A report could then be written detailing the changes made and advice given. More traditional testing techniques which appropriately sample knowledge are also acceptable.

Another approach to assessment would be the creation and maintenance of a web log, which would record candidate activity throughout the Unit. This would log, on a daily or weekly basis, what candidates learn and what they do. However, their posts would have to satisfy the relevant Performance Criteria. Practical activities could also be recorded *via* the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post). 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) carried out by the learner during the life of the Unit.

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the statements, identifications, descriptions and selections necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, etc that collectively evidence candidates' competencies. Some form of authentication would be required. This could be as simple as a statement of originality, signed by the candidate and the assessor.

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

In this Unit, learners will have the opportunity to develop some of the following Core Skills:

Information and Communication Technology (SCQF level 4)
Communication (SCQF level 4)
Working with Others (SCQF level 4)

ICT skills in particular will be useful, with a particular focus on data and data security. There will be opportunities to understand online systems and the way they store, process and use information.

Communication skills can be developed during this Unit, depending on the methods of assessment selected; group presentations and the opportunity to work with others could complement this.

History of changes to Unit

Version	Description of change	Date

General information for learners

Unit title: Data Security (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 improve your knowledge of data security. It will also help you be aware of the importance of keeping your personal data secure online, and methods for doing this.

This Unit covers the basics of what data is, where it is stored and how it can be used online by you and by others. Also, the implications of sharing data, and potential risks associated with this are covered, including examples of situations where data sharing can go wrong.

It also shows how you can keep your own data safe online, with a range of methods for practising 'good data security'.

The Unit is designed for beginners, and no previous knowledge or experience of computers is presumed. It is designed for the beginner who wants to learn the basics of data security. The main aim of this Unit is to teach you about how your own personal data can be used online and how to be responsible for what data you choose to share online.

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

- What data is.
- Where data is stored.
- How personal data is used online.
- Risks associated with sharing personal data online.
- Negative consequences of data sharing.
- General principles of keeping your personal data secure.

This Unit is part of a series of Units on data security. You may progress to the *Data Security* Unit at SCQF level 5 on completion of this Unit if you wish to improve your knowledge and skills in this area.

You will be assessed on the knowledge and skills covered in this Unit. The assessment of this Unit may take different forms. You may, for example, sit a short test of your knowledge and carry out some practical tasks. The assessment will be straightforward and will not take much time.

You may also develop skills that may lead to employment, skills in sustainable development and citizenship skills during your learning experience.