bcs

The
Chartered
Institute
for IT

Qualification Specification Guide

BCS Level 1 Award in e-Safety

Version V2.2 August 2019

These are qualifications which are regulated by one or more of the following: Ofqual, Qualifications Wales, CCEA Regulation or SQA

Contents

1. Introduction to the Qualification 3

1.1 Qualification Objectives 3
1.2 Who the Qualifications are for? 3
1.3 Entry Requirements 3
1.4 Learner Progression 3
1.5 Qualification Size 3

2. Structure and Content 4

2.1 Structure of the Qualification 4
2.2 Guidance on the Unit Content 4
2.3 Learning Outcomes and Assessment Criteria 5

3. Assessment 7

3.1 Summary of Assessment Methods 7
3.2 Grading 7
3.3 Availability of Assessments 7
3.4 Externally Assessed Units 7
3.5 Specimen Assessment Materials 7
3.6 Support Materials 8
3.7 Access to Assessment 8

4. Contact Us 8

Appendix: Qualification Level Descriptors 9
Useful Links 9

1. Introduction to the Qualification

1.1 Qualification Objectives

BCS Level 1 Award in e-Safety from BCS, The Chartered Institute for IT is designed to help schools deliver e-Safety through curriculum in a variety of subjects and improve standards of safety amongst learners. In qualifying in this subject, learners are being alerted to potential dangers and working towards essential positive changes in behaviour.

1.2 Who the Qualifications are for?

Designed specifically for learners in key stage 3 and 4, e-Safety is aligned to the national curriculum and offers practical solutions to other issues that may be encountered in day-to-day life.

1.3 Entry Requirements

There are no pre-requisites that a learner must achieve prior to taking this e-Safety qualification, all knowledge, skills and understanding about the subject will be covered within the training.

1.4 Learner Progression

The BCS Level 1 Award in e-Safety qualification has been designed to incorporate the ITQ unit Internet Safety for IT Users (H/502/9154).

This qualification and its credits (3 credits) can be used to contribute towards a larger ITQ qualification.

1.5 Qualification Size

The size of the qualifications are described in terms of Guided Learning Hours (GLH) and Total Qualification Time (TQT).

GLH indicates the approximate time (in hours) that the learner will be supervised during any teaching, learning or assessment activities.

TQT is a predication of the total time a learner with no prior knowledge might need to complete the course.

TQT is made up of two elements: GLH, and all other hours (an estimate of the number of hours a learner will reasonably spend on any unsupervised learning or assessment activities including homework, research, exam preparation and formal assessment) so that they can successfully achieve the qualification.

The qualification requires the following GLH and TQT:

Qualification Title	QAN	Accreditation Start	GLH	TQT
BCS Level 1 Award in e-Safety	600/0830/1	1 March 2011	29	37

2. Structure and Content

2.1 Structure of the Qualification

To gain the BCS Level 1 Award in e-Safety, learners must complete this 1-unit qualification.

The qualification covers four main areas:

- The benefits and risks of using the internet
- How to report and respond to e-Safety issues
- How to protect yourself and your computer online
- The legal issues of downloading from the internet

On completion, learners will gain a certificate to show they have successfully completed the course, but they will also be award with 3 credits (ITQ) which can be used to gain further ITQ qualifications.

2.2 Guidance on the Unit Content

The Internet Safety for IT Users (H/502/9154) unit assesses the skills and knowledge required by the IT user to work safely and responsibly online. As a result of this unit, IT users will understand the risks of working online and be able to take appropriate precautions to safeguard themselves and others.

2.3 Learning Outcomes and Assessment Criteria

Learning outcomes **The learner will...**	**Assessment criteria** **The learner can...**	**Examples**
1. Understand the risks that can exist when using the Internet.	1.1 Identify risks to user safety and privacy.	User safety and privacy (e.g. abusive behaviour [“cyberbullying”], inappropriate behaviour and grooming, abuse of young people, false identities, financial deception)
	1.2 Identify risks to data security.	Risks to data security (e.g. theft of data, hacking, accidental deletion or change to data, Trojans, spyware, adware, phishing, identity theft, avatars, mobile technology – wireless and Bluetooth, default passwords, portable devices – USB devices)
	1.3 Identify risks to system performance and integrity.	Risks to system performance and integrity (e.g. unwanted email – often referred to as “spam”, worms, viruses, spyware, adware, denial of service, hacking of systems, Trojans, spam)
	1.4 Outline how to minimise Internet risks.	Minimise Internet risks (e.g. virus-checking software, anti-spam software, firewall, treat messages files software and attachments from unknown sources with caution, internet settings, block sites, parental controls)
	1.5 Outline factors that affect the reliability of information on websites.	Reliability of information on websites (e.g. accuracy, currency, sufficiency, synthesise information from a variety of sources, recognise intention and authority of provider, bias, level of detail, relevance)
2. Know how to safeguard self and others when working online.	2.1 Take appropriate precautions to ensure own safety and privacy.	Precautions to ensure own safety and privacy (e.g. selection and management of username, password or PIN, including reasons for changing passwords or PINs, length and complexity of passwords, online identity profile, access levels of information, confidentiality content filtering, proxy servers, monitoring and reporting user behaviour)
	2.2 Protect personal information online.	Protect personal information online (e.g. username and password/PIN selection and management, password strength, online identity/profile, real name, pseudonym, avatar, what personal information to include, who can see the information, withhold personal information)
	2.3 Carry out checks on others online identity.	
	2.4 Describe the forms and features of cyberbullying.	Cyberbullying (e.g. chat rooms, email and instant messaging)
	2.5 Identify when and how to report online safety issues.	Report online safety issues (e.g. abusive behaviour [“cyberbullying”], inappropriate behaviour and grooming, abuse of young people, false identities, financial deception)
	2.6 Identify where to get online help and	

Learning outcomes The learner will...	Assessment criteria The learner can...	Examples
	information on e-Safety.	Help and information on e-safety (e.g. service provider, legal system, parental controls) Legal constraints on the uploading and downloading of software and other digital content (e.g. relating to copyright, software download and licensing, digital rights, IPR, Health and Safety, Children Legislation, Data Protection) Precautions to maintain data security (e.g. use access controls, configure anti-virus software, adjust internet security settings, carry out security checks, report security threats or breaches, backup, store personal data and software safely, treat messages files software and attachments from unknown sources with caution, proxy servers, download security software patches and updates, Loss or theft of valuable and possibly irreplaceable data, cost of replacing lost data, a range of effective backup procedures) Precautions to maintain system performance and integrity (e.g. set passwords, physical access controls – keypads or locks, anti- virus software, adjust firewall settings, carry out security checks, report security threats and breaches, back up data and software and store appropriately, identify and report possible security threats, download and install software patches and updates, treat messages files software and data from unknown sources with caution, proxy servers) Browser safety and security settings (e.g. autofill, cookies, security, pop-ups, appearance, privacy, search engine, toolbars, personalisation, accessibility, software updates, temporary file storage) Guidelines and procedures for the safe use of the Internet (e.g. set by employer or organisation relating to Health and Safety, security, equal opportunities, disability)
3. Take precautions to maintain data security.	3.1 Take appropriate precautions to maintain data security.	
	3.2 Take appropriate precautions to maintain system performance and integrity.	
	3.3 Use appropriate browser safety and security settings.	
	3.4 Use appropriate client software safety and security settings.	
4. Follow legal constraints, guidelines and procedures which apply when working online.	4.1 Identify legal constraints on the uploading and downloading of software and other digital content.	
	4.2 Identify legal constraints on online behaviour.	
	4.3 Correctly observe guidelines and procedures for the safe use of the Internet.	

3. Assessment

3.1 Summary of Assessment Methods

For this qualification, learners will be required to complete a short automated assessment that demonstrates the learning outcomes and assessment criteria have been met.

The assessment is a 30 minute test which comprises of:

- 28 questions
  - 19 multiple choice questions
  - 9 simulation questions
- 75% pass rate

Guided Learning Hours – 29 hours (classroom based).

Internet Safety for IT Users is part of the ITQ framework, therefore the assessment strategy for the BCS Level 1 Award in e-Safety qualification conforms to the ITQ Assessment Strategy.

3.2 Grading

BCS Level 1 Award in e-Safety is a pass / fail qualification. To pass the qualification, learners must achieve 75% for more to gain the certificate.

3.3 Availability of Assessments

As the assessment of the BCS Level 1 Award in e-Safety qualification is delivered through an automated assessment, the centre will require access to the learner management system which carries no specific system requirements.

3.4 Externally Assessed Units

An invigilator will need to be present to ensure exam conditions are observed. Those currently registered to invigilate the ECDL/IT user assessments will also be permitted to invigilate the assessments for this qualification.

3.5 Specimen Assessment Materials

Specimen assessments are available using the automated assessment method and will be made automatically available to learners.

3.6 Support Materials

BCS provides the following resources specifically for this qualification:

Description	How to access
20 Lesson Plans, presentation, worksheets and activities	Purchased through BCS
e-learning package (year 7)	Purchased through BCS

Learners can access a wealth of support information about online safety, these include:

CEOP	http://ceop.police.uk/
ThinkuKnow	http://www.thinkuknow.co.uk/
BeatBullying	http://www.beatbullying.org/
Kid Smart	http://www.kidsmart.org.uk/

3.7 Access to Assessment

BCS will endeavour to provide equal Access to Assessment for all learners, ensuring that there are no unnecessary barriers to assessment and that any reasonable adjustments for learners preserve the validity, reliability and integrity of the qualification.

Requests for reasonable adjustments will be managed by the Centre and considered by BCS to ensure they meet the legal regulatory requirements. Further information about our access to assessment policy can be found on the Approved Centre Forum.

4. Contact Us

BCS is committed to providing you with professional customer service and support. Please see how to contact us by clicking on this link: https://www.bcs.org/contact-us/.

If you require this document in accessible format, please contact us.

Appendix: Qualification Level Descriptors

Level 1

Knowledge

The holder

- has basic factual knowledge of a subject and/or knowledge of facts, procedures and ideas to complete well-defined routine tasks and address simple problems;
- is aware of aspects of information relevant to the area of study or work.

Skills

The holder can

- use basic cognitive and practical skills to complete well-defined routine tasks and procedures;
- select and use relevant information;
- identify whether actions have been effective.

Useful Links

If you're interested in delivering our qualifications, further information is available on our website: https://www.bcs.org/deliver-and-teach-qualifications/become-accredited/

Approved Centre Forum: https://tcforum.ecdl.co.uk/tcforum/