WJEC Level 1/2 Vocational Award in ICT (Technical Award)

Guidance for Teaching

Unit 1 Guide

Aims of the Guidance for Teaching

The principal aim of the Guidance for Teaching is to support teachers in the delivery of the WJEC Level 1/2 Vocational Qualification in ICT (Technical Award) and to offer guidance on the requirements of the qualification and the assessment process. The Guidance for Teaching is **not intended as a comprehensive reference,** but as support for professional teachers to develop stimulating and exciting courses tailored to the needs and skills of their own learners in their particular institutions.

Aims of the Unit Guide

The principal aim of the Unit Guide is to support teaching and learning and act as a companion to the Specification. Each Unit Guide will offer detailed explanation of key points in the Specification and aim to explain complex areas of subject content. An overview of the whole course can be found in the Delivery Guide.

© WJEC CBAC Ltd.

CONTENTS

© WJEC CBAC Ltd.

Introduction

The WJEC Level 1/2 Vocational Award in ICT (Technical Award), approved by Ofqual and DfE for performance qualification tables in 2024 (first teaching from September 2022), is available to:

- all schools and colleges in England and Wales
- subject to local agreement, it is also available to centres outside England and Wales, for example in Northern Ireland, the crown dependencies of the Isle of Man and the Channel Islands, and in British overseas territories, and to British forces schools overseas. It is not available to other overseas centres.

It will be awarded for the first time in January 2024, using grades Level 1 Pass, Level 1 Merit, Level 1 Distinction, Level 1 Distinction*, Level 2 Pass, Level 2 Merit, Level 2 Distinction, Level 2 Distinction*.

Additional ways that WJEC/Eduqas can offer support:

- sample assessment materials and mark schemes
- face-to-face CPD events
- examiners' reports on each question paper
- free access to past question papers and mark schemes via the secure website
- direct access to the Subject Officer
- free online resources
- Exam Results Analysis
- Online Examination Review
- Regional Support team (England Centres only).

© WJEC CBAC Ltd.

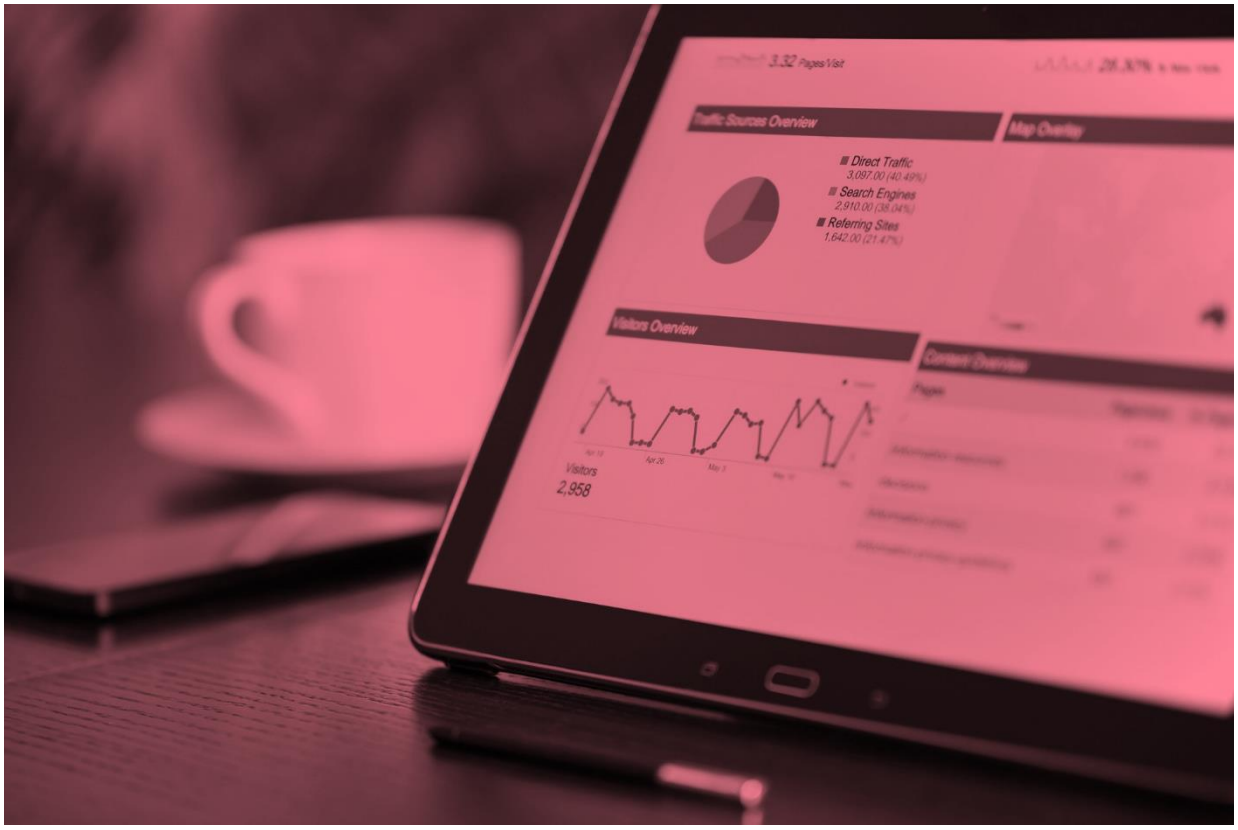
Overview of Unit 1

Unit 1: ICT in Society
(40% of the qualification)

Overview of the unit

Unit 1 allows learners to explore the wide range of uses of hardware, application and specialist software in society. They will investigate how information technology is used in a range of contexts, including business and organisations, education and home use.

1.1	How IT can be used to fulfil the needs of organisations and individuals
1.2	How data and information is used and transferred
1.3	Legal, moral, ethical, cultural and environmental impacts of IT and the need for cybersecurity



© WJEC CBAC Ltd.

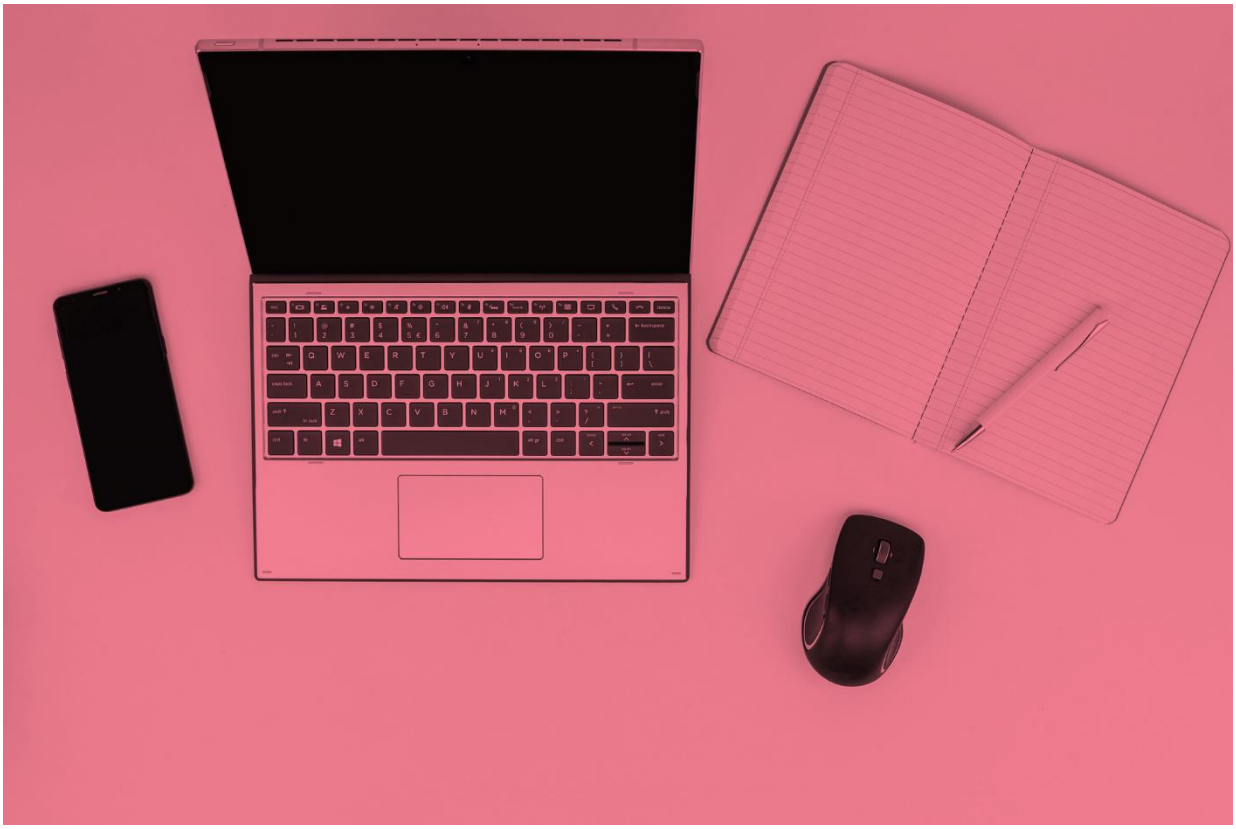
How to read the Specification

WJEC/Eduqas Vocational Award (Technical Awards) specifications are written to be transparent and easy to understand.

The amplification provided in the right-hand column uses the following four stems:

- 'Learners should know' has been used for the recall of facts such as: legislation and definitions.
- 'Learners should know and understand' has been used for the majority of the unit content where knowledge needs to lead to a sense of understanding.
- 'Learners should be aware of' has been used when the volume of content is quite extensive, and learners do not need to understand all aspects in detail.
- 'Learners should be able to' has been used when learners need to apply their knowledge to a scenario or practical situation.

The amplification provided includes all of the assessable content for the relevant section, unless it states, *'e.g.' 'including'* or '*such as'*. In these cases, the amplification lists relevant content, which should be expanded upon in an appropriate way, taking account of learners' needs and interests. The use of the word '*including*' indicates compulsion (i.e. a question could be specifically set on that aspect). The use of the words *'e.g.'* or *'such as'* are for guidance only, and an alternative can be chosen.



© WJEC CBAC Ltd.

UNIT 1 TEACHER GUIDANCE

1.1 How IT can be used to fulfil the needs of organisations and individuals		
Content Amplification		**Teacher Guidance**
1.1.1 Functionality of different hardware devices	Learners should know and understand types of: • computing devices • input devices • output devices • storage devices • basic internal components ports.	This is a good introduction to the course, as it builds on the knowledge that learners have gained during KS3. They will already be familiar with a range of input, output and storage devices but they may be less familiar with basic internal components such as ports. Learners should not only be able to recognise various hardware devices, but they should also understand their function both for personal use and for business use.
1.1.2 Functionality of different software	Learners should know and understand: • system software • applications software • utility software • specialist software • information handling software • open source software • communication software.	Learners should already understand the concept of software and will appreciate the function of packages known to them. In the KS3 curriculum learners learn about system, application and utility software, which is key to operating a stand-alone or network system computer or another device (e.g., phone). They are now required to extend their knowledge to being able to understand the range of software that is available with a wider knowledge for business use. This knowledge also allows learners to understand the use of software for analysing and evaluating data sets and improving productivity in relation to time/resource management. This will enable learners to be able to fix simple software malfunctions and maintain software.
1.1.3 Services provided by IT	Learners should be aware of how each service improves efficiency/productivity for businesses and/or individual users: • Smart TV • gaming • image capture and manipulation • webcam services	Learners will already be aware of many of the services provided by IT but may not have previously considered how each service could improve efficiency and productivity. Learners should be taught how they personally can take advantage of IT services for leisure and recreation to help them organise their finances, schedules and activities. They also need to understand how these services improve efficiency and/or productivity commercially as this will both improve their understanding and prepare them for the world of work. This topic could be introduced in a brainstorming session, with learners creating mind maps to explore the benefits of each of the services listed.

© WJEC CBAC Ltd.

	• social networking: information needed to create accounts; services available • music and sound including downloading from the Internet and related issues • mobile phones • banking • E-commerce systems • payroll • modern mail handling methods • control processes (feedback) • robotics and bionics • artificial intelligence (AI) and expert systems • online shopping and searching for products on websites • booking online • registration systems • management information systems • weather forecasting systems • remote storage technologies • online education and blended learning • security systems • accessibility • virtual reality and augmented reality • 3D Printing • wearable technologies • cloud computing • disabled accessibility • emerging technologies.	Learners also need to learn about potential future developments and emerging technologies in technology, including AI and expert systems, to give them awareness of the future world they will be living in.

© WJEC CBAC Ltd.

UNIT 1 TEACHER GUIDANCE

1.2 How data and information is used and transferred		
Content Amplification		**Teacher Guidance**
1.2.1 Why data must be fit for purpose	Learners should know and understand: • that data consists of raw facts and figures • that information is data which has been processed by the computer • that knowledge is derived from information by applying rules to it • the need for good quality data • the potential benefits of encoding data and the reasons for doing it • improvements in speed of access to data and increased storage • advantages and disadvantages of using information and communication technology for storing data • file types • data compression • file properties.	Learners need to understand how data becomes information, and information, when rules are applied to it, becomes knowledge, which can be used for a specific purpose. Understanding the need for accurate data is imperative as learners need to learn to be more accurate and exact in everything they do. The idea of GIGO (Garbage In, Garbage Out) is a valuable concept for learners to appreciate. Learning about good quality and valid data will help them to make better judgements regarding fake news and research they may undertake, giving them a more critical thinking way of looking at information. Learners should also understand the cost of information as part of quality information to help them understand how good quality and accurate data is crucial to the success of a business. Learners also need to understand methods of data transfer, including encoding, in order to understand how personal and business data can be affected. This is important so that learners can understand the security, storage and validity of data in a business and personal use. Understanding different file types and compression will allow learners to decide how data can be used by others and possibly what programs will be able to access that data.
1.2.2 How input data is checked for errors	Learners should know and understand: • data capture methods • methods used for validation and verification and where they are appropriate • possible sources of error which could exist • techniques used to overcome these errors.	Ask your learners if they know of any data capture methods. By a show of hands, your learners will have taken part in data collection and this could well be a good starting point for this topic. Although this will not be a good example of commercial data capture, other methods such as surveys or bar codes will be familiar territory on which to build their knowledge. Learners must understand the methods used for validation and verification, where they are appropriate and how these can be applied within businesses. The theory for validation and verification could be reinforced during the practical database task for Unit 2. Building on the importance of data accuracy from the previous section, learners should consider possible sources of error and which techniques are available to overcome these errors. They might

© WJEC CBAC Ltd.

		consider techniques that they have come across themselves, such as data validation on online forms and verification of passwords to gain access to websites.
1.2.3 How data transfers over different types of network	Learners should know and understand: • the differences between local (LAN) and wide area (WAN) networks • the purpose of protocols • computer network operation • network topologies including bus, star and ring • internet/extranet/intranet • devices within a network • how data is transferred over a network • potential threats to data transfer (e.g. packet sniffing) • cloud computing vs in-house servers • emerging technologies.	Understanding more about networks builds on the KS3 curriculum and goes on to develop a deeper understanding of how businesses, centres and homes can use the different types of networks. Learners should understand the differences in types of network and topologies and have an awareness of potential threats to data transfer as this will enable them to make choices about how to protect data. This content aims to enable learners to be able to measure the threats to physical hardware, specific types of topologies, and obstructions/threats to data when transferred or stored. Learners should learn about a variety of types of network as they are likely to be required to apply their knowledge to a specific scenario when sitting the examination. New technologies in data transfer are constantly emerging and learners should be alert to these, so their knowledge of data transfer remains current.
1.2.4 Different types of connectivity	Learners should know and understand: • connection methods • short range wireless connection (802.11 Bluetooth), near-field communication (NFC) and radio-frequency Identification (RFID) • medium range wireless connection (3G/4G/5G) • long range wireless connection (microwave, satellite) • ethernet, USB, micro USB and USB C • emerging technologies.	How devices connect with each other can make a significant impact on connection experience, therefore learners should understand the options available to them so they can make an informed decision on what type of connection to use in a range of situations. The different ways to connect has become increasingly important to learners with the use of mobile phones – they understand more about data usage and especially when living in a rural setting (wireless v Ethernet) – and so this might be a good starting point for this section. Knowing more about data and transferring data will help learners understand the different types of connectivity that are crucial to business. Understanding these will help learners make informed choices for the most efficient or cost-effective connection method for their needs. Learners should also be encouraged to keep their learning current by following new developments and emerging technologies.

© WJEC CBAC Ltd.

UNIT 1 TEACHER GUIDANCE

1.3 Legal, moral, ethical, cultural and environmental impacts of IT and the need for cybersecurity		
Content Amplification		**Teacher Guidance**
1.3.1 Risks to information held on computers	Learners should know and understand: • accidental damage • unintended disclosure by incorrectly assigned access levels • malicious software including viruses, worms, Trojan Horses, spyware, ransomware, DDoS and key logging • hacking (e.g. white, black and grey hat) • social engineering • emerging threats.	Learners should be aware of how they themselves could accidentally lose data, as well as understanding threats from outside of their system, which might include malicious software, hacking and social engineering. This section will enable learners to understand the importance of backing up work, sharing personal details in limitation and only when necessary, having different security passwords for different uses/platforms and so on. Beyond the concept of hacking, learners should be introduced to the concept of ethical hacking and penetration testing in order to develop an understanding of how companies deal with threats to data and privacy. Learners should also be aware of a range of common attacks, alongside emerging threats, as these are the ones they are likely to face in the workplace. This will help learners to be vigilant and keep their information safe. It is only by being aware of these risks that learners will be able to take steps to prevent data loss. Learners should research emerging threats and relevant current news items should be discussed in class as this will help when applying their knowledge to scenarios in the written examination.
1.3.2 The impact of data loss, theft or manipulation on individuals and businesses	Learners should know and understand: • financial implications • moral and legal implications (including competitor advantage, breaking of GDPR/DPA, open to blackmail) • data manipulation • loss of service • loss of intellectual property • loss of reputation.	By learning about the impact of data loss, theft or manipulation on individuals and businesses, learners will understand the importance of being vigilant when working with data. From a vocational context, the protection of data is fundamental to ensuring good quality data and the success of a business. The financial implication is the difference between success and failure of a company and ensuring they understand this area will help learners make better decisions with the knowledge gained from the previous sections on the importance of data. Learners may be asked to consider the impact of data loss, theft or manipulation on individuals or organisations in the written examination.

© WJEC CBAC Ltd.

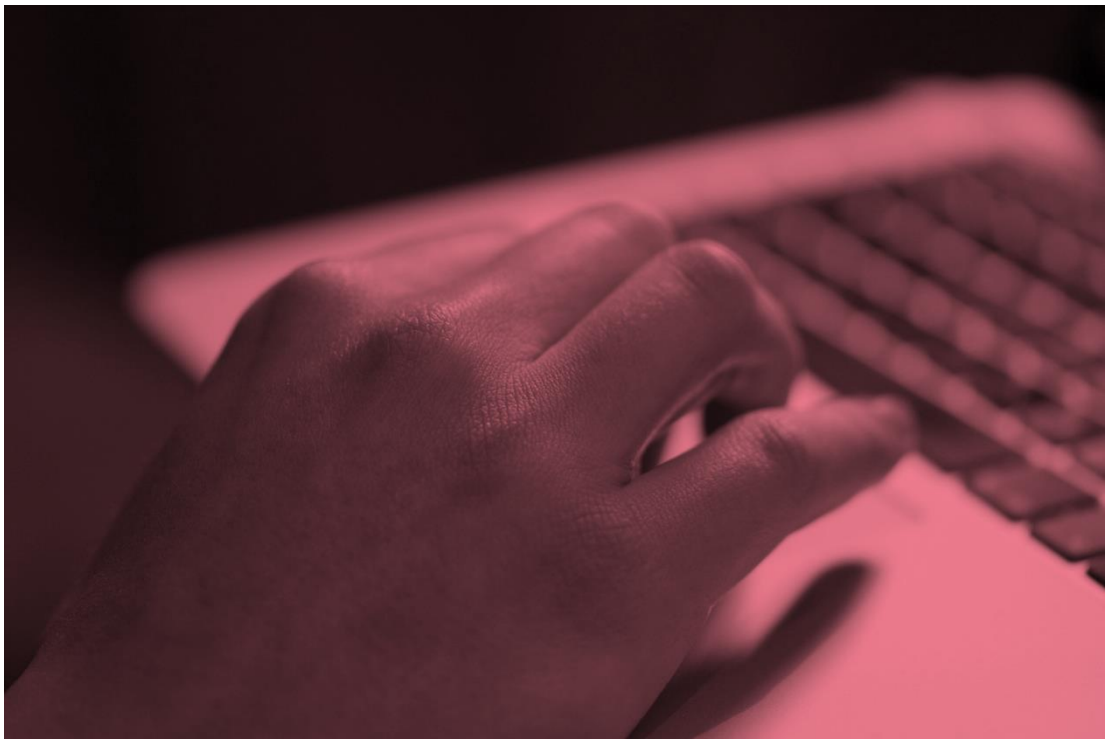
1.3.3 Methods used to protect information	Learners should know and understand: • logical protection including access levels, authentication, firewalls, anti-malware applications, password protection and encryption • physical protection including locks, biometrics, location of hardware, backup systems and security staff • security policies including disaster recovery, staff responsibilities, acceptable use policy and staff training • emerging technologies.	With an understanding of the potential consequences of data loss, learners will appreciate the need to arm themselves with a range of methods with which to protect their information. This will include knowledge of both logical and physical protection methods available, including any new developments. Learners also need to appreciate how companies will have security policies in order to minimise the threat to information stored and this will encourage learners to follow these policies when they start out in the workplace. Standard and common-sense working habits should be adopted in the workplace; for this to happen, learners need to be educated about how these measures can be implemented at organisation and individual level. Learners will have to follow a security policy when using the centre computer network. However, they are likely to have limited knowledge of logical and physical protection systems from their experience of using computers at their centre and at home. This is an area that is constantly developing, and learners should be encouraged to keep up to date with new protection methods.
1.3.4 How moral and ethical issues affect computer users	Learners should know and understand: • privacy and security • cookies and data collection by multinational companies • monitoring of individuals • impact of data loss or damage.	Learners should have an understanding of moral and ethical issues that affect computer users in order for them to make informed judgements about what is right and wrong. This builds on 1.3.3 where learners must understand the fine line between freedom and responsibility. Learners need to be aware of what cookies are and how they are used to increase brand awareness, whilst considering in what ways their use could affect the more vulnerable population in a negative way. Whilst privacy is protected by a range of measures, learners must understand when a company may want to monitor an individual. They should consider the issue from both the side of the individual worker and that of the company managers.
1.3.5 How legal issues protect computer users	Learners should know: • General data protection regulation (GDPR) 2018 • Data protection act (DPA) 1998 • Computer misuse act 1990 • Communications act 2003 • Regulation of investigatory powers act 2016	Learners need to know how legal issues protect computer users so that they understand the parameters and can operate within the law, as well as having an appreciation of how legislation protects their own rights. Teachers may wish to introduce the subject with a quiz to test the initial knowledge of their learners. Practical activities such as card matching might help to make this topic more appealing. Once the content has been delivered, learners could make their own quizzes and test each other to test their knowledge.

© WJEC CBAC Ltd.

	• Copyright, designs and patents act 1988 • Health and safety legislation.	
1.3.6 The cultural, personal and environmental impact of ICT	Learners should be aware of: • employment patterns • retraining • changes in working practices (e.g. collaboration, hot desking) • teleworking • homeworking • videoconferencing • effect on transport • effect on traditional media • drones • green IT and non-green IT • e-waste • rare earth element mining • global production lines • the digital divide – local and global • social media including cyberbullying and Fake News • net neutrality • addiction • mental health • emerging technologies.	This topic is probably best approached as a discussion, learners could share their knowledge of the bullet points from this section. Learners could research topics, either individually or in groups, and then report their findings to each other. The Covid 19 pandemic revealed how working remotely can replace the physical presence in the workplace; with this comes a wide array of tools. From videoconferencing to finding a work-life balance, which may involve a better quality of life due to the lack of commute, learners need to develop an understanding of the pros and cons of homeworking, including the digital divide and access to technology. ICT has an impact on almost every aspect of our lives – from working to socialising, learning to playing. The digital age has transformed the way young people communicate, network, seek help, access information and learn. With environmental issues gaining more and more international attention, learners should appreciate the potential impact of areas such as green IT and non-green IT, e-waste and rare earth element mining. Fake News, cyberbullying and mental health are also hot topics and should be investigated and discussed in the context of ICT impact. Learners should be encouraged to take an interest in the cultural, personal and environmental impact of ICT by discussing news items, documentaries and television programmes such as 'Click'.

© WJEC CBAC Ltd.

1.3.7 How a digital footprint can impact computer users	Learners should know and understand the potential effects of: • digital footprint – passive and active • posts on social media • online identity • identity theft • the risks of inappropriate images.	Understanding the effects of their digital footprint will help learners choose and control what they leave online for others to find. This knowledge will help learners avoid risks such as identity theft and teach them that leaving a positive digital footprint can be beneficial to their reputation and future opportunities. Through understanding the impact of their digital footprint, learners will be better able to make informed choices about the information they share online. Learners could investigate case studies that illustrate how a digital footprint can impact upon people, both positively and negatively. They could also produce their own set of guidelines for creating a positive digital footprint



© WJEC CBAC Ltd.

CREATE YOUR OWN EXAM QUESTIONS

When you are helping your learners prepare for Unit 1 you will find using the questions in the SAMs useful. However, we appreciate that at the start of a course you might want to have a bigger bank of questions to use with you students. Therefore, you might find it useful to create some of your own. You might even decide to get your students to write their own questions and mark schemes. This step-by-step guide will help you create your own exam papers.

All exam questions have three core elements:

A command word + **Link to the specification content** + **A tariff**

What do you need to know about the core elements?

Command word	1. Must be appropriate for the task. 2. Must be linked to the assessment objective. 3. Are often linked to the question's tariff.	1. Is it clear to the learner what they are expected to do in order to access the full range of the mark scheme? 2. If the question is targeting more than one assessment objective, more than one command word must be used. **A full table of how command words relate to assessment objectives is available in the 'Assessment Guide'.** 3. For example, commands words such as 'state' and 'name' should be reserved for lower tariff questions, whereas 'analyse' and 'explain' are often better for higher tariff questions.
Link to the specification content	1. The question must ask the learner about content listed in the specification only. 2. The link to the specification must be clear and unambiguous.	It should be clear which area/s of the specification are being targeted. Consider the stem of the specification content and this will indicate the depth the learner should know and understand the content.
Tariff	1. Must be appropriate for the command word used. 2. Must be appropriate for what is being assessed. 3. Must be accessible for level 1/2 learners within an exam context.	1. It should be possible and clear to the learner how they can achieve all of the marks available for any question: the higher the tariff, the longer the learner should take to answer the question. A good starting point is to allow one mark per minute. 2. Use the SAMs as a guide for what is an appropriate tariff and about the range of tariffs used across a whole paper.

© WJEC CBAC Ltd.

Name three different types of computing devices that customers might use to play games. [3]

Command word | **Unambiguous link to specification** | **Tariff**

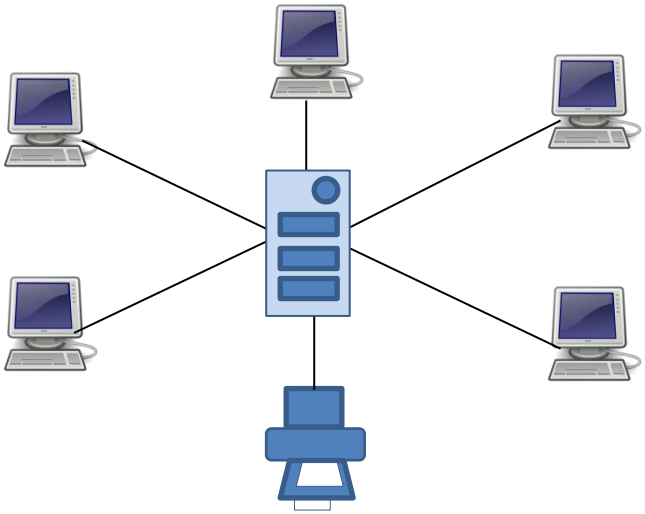
There are some additional elements that some exam questions use:

Context	As this is a Vocational Subject, our ICT papers start each question with a short scenario. All sub questions then relate back to this scenario. These scenarios are relatively short (approximately 30-50 words) and tend to feature a company or individual who is using ICT.	A context should be written clearly and using language that is as simplistic as possible. The context should be concise and should provide only the information that learners will need to answer the question. Additional information may be time-consuming or misleading. It should depict something that learners will understand, rather than something that is unfamiliar or confusing. **An example of a question that uses a context is question 3 from the Unit 1 SAMs:** 3. Alisha runs a dog-walking business from home. She has a PC and an all-in-one printer. Alisha lives in a small village where broadband connection is not available. As she is far away from the local town, she likes to take advantage of online services to help run her business.

© WJEC CBAC Ltd.

1. *Stock 'em Up Stores* is a supermarket chain with shops throughout the country. Each store has its own Local Area Network (LAN) and this connects to the central office using a Wide Area Network (WAN).

   The LAN layout of the network topology in each store is similar to the one shown below.



© WJEC CBAC Ltd.

Assessment Objectives

Each question should target an assessment objective which is signalled by the command word. If more than one Assessment Objective is targeted, more than one command word should be used.

A full table of the assessment objectives that have been set for all our Vocational qualifications is available in the 'Assessment Guide'. However, what does each assessment objective require learners to do?

AO1	Requires learners to recall the knowledge that they have learned throughout their course.
AO2	Requires learners to: • use learned material in a new situation with a minimum amount of help or direction • apply rules/principles to a problem, without being given the rule; problem solving.
AO3	Requires learners to: • break material into component parts so that its structure may be understood • break complex concepts down to component parts and analyse how parts are related to each other; seeing patterns, recognising hidden meanings • judge the value of material based on certain criteria • evaluate, make judgments on the worth of a concept for a purpose • resolve controversies/differences of opinion • verify value of evidence • recognise subjectivity.

© WJEC CBAC Ltd.

What type of question should be used?

There are several ways to ask a question, and you should consider what is most appropriate for the question that you're asking. Some guidance is given below:

Matching pairs Multiple choice True or false	These styles of question are useful for asking questions that have answers that are predetermined, usually assessing straightforward knowledge and understanding (AO1).	These questions should be marked objectively, in that there is a correct and an incorrect answer. **For an example, see page 5 of the SAMs.**
Short Answer	These can be open-ended and require learners to construct a short answer. They are low tariff, and usually used to test knowledge and understanding. Short answer questions are also used for calculations and data manipulation.	This type of question could be marked objectively if there is one or several correct that might be given. However, if the candidate is required to construct a response, it may be that subjectivity is required to decide whether a number of marks maybe given according to the accuracy and quality of the response, as permitted by the tariff. **For an example, see page 6 of the SAMs.**
Extended answer	This allows learners to respond at length to open-ended questions. In this, learners may be required to organise their ideas, to build an argument, and may result in a range of interpretations that draw upon wider and more flexibly defined sources. These are usually used to test higher skills, writing and structuring skills, further reading and a deeper level of understanding.	These questions will be marked subjectively: you should use your judgement to place learners' responses into bands that detail criteria that responses should meet. **For an example, see page 8 of the SAMs.**
Problem solving	These require a range of critical thinking skills from identification, description and analysis, to synthesis and evaluation. Sometimes there will be exact or correct answers to problems – as in answering maths problems – or sometimes learners may be asked to propose and justify a course of action to address a specified situation, or to develop a well-reasoned explanation or response based on data analysis, models or precedent.	Questions that require exact or correct answers should be marked objectively, in that there is a correct and an incorrect answer. Questions that require a proposed or justified course of action will be marked subjectively: you should use your judgement to place learners' responses into bands that detail criteria that responses should meet.
Graph production or interpretation	Graph production questions involve both numerical/mathematical skills. Graph interpretation questions involve both numerical/mathematical skills as well as reasoning skills.	These questions should be marked objectively, in that there is a correct and an incorrect answer. **For an example, see page 13 of the SAMs.**

© WJEC CBAC Ltd.

Golden Rules:

1. Try and keep questions as short and clear as possible.
2. Consider splitting long questions into a statement and a question.
3. Avoid asking more than one question in a sentence.
4. Use plain English, e.g., *buy* rather than *acquire.*
5. Avoid using:
   a. negatives (where possible)
   b. technical language (unless it is part of what is being assessed)
   c. idioms/metaphors/non-literal use of language, e.g., see eye to eye, cut back on, branching out
   d. words that have more than one meaning, e.g., volume, fit, illustrate (unless it is part of what is being assessed)
   e. gender-biased words, e.g., chairman, manmade, policewoman.
6. Across a whole paper, questions should increase in difficulty. Higher tariff questions are more likely to be found towards the end of the paper.
7. A whole paper should sample a wide range of specification content. You might find it useful to use a blank version of the tracking grid from the Unit 1 SAMs (page 36).

© WJEC CBAC Ltd.

Terminal Rule

Key Principles:

Candidates must take the external assessment, worth 40% of the qualification, in the series in which they certificate. This is the examined unit in all qualifications so for ICT this is Unit 1.	Only the result for the external assessment that are achieved in the final series, the series in which candidates 'cash-in', can contribute to their final grade. If a candidate takes the external assessment prior to the series in which they 'cash-in', this result cannot contribute to the overall grade, even if it is the better result.	In relation to performance table points – as opposed to individual candidate results – it is always the first qualification result which counts, irrespective of whether a candidate re-certificates again at a later date.

- Candidates can enter for internally assessed units in January and June
- Candidates may resit each **internally** assessed unit but cannot improve previously submitted work. The best uniform mark score from the attempts will be used in calculating the final overall grade.

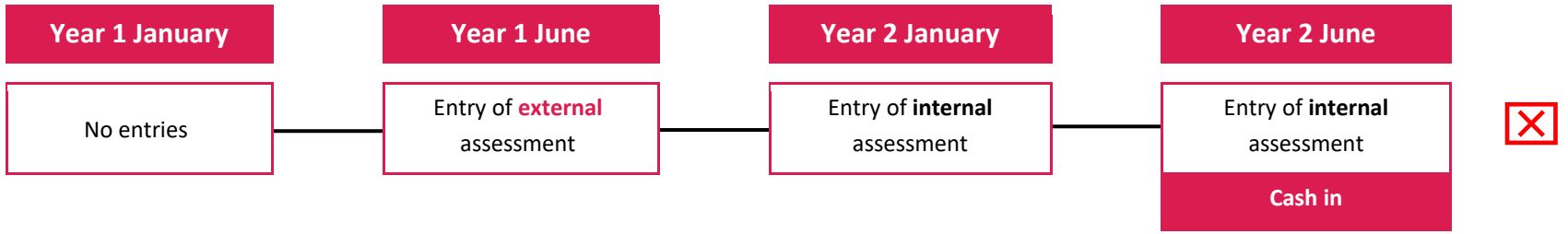
Example scenarios (assuming that the delivery of the qualification takes place over two years):

Scenario 1:

Year 1 January	Year 1 June	Year 2 January	Year 2 June	
No entries	Entry of **internal** assessment	Entry of **internal** assessment	Entry of **external** assessment **Cash in**	✓ Entry for external assessment takes place in the same series as cash-in and certification.

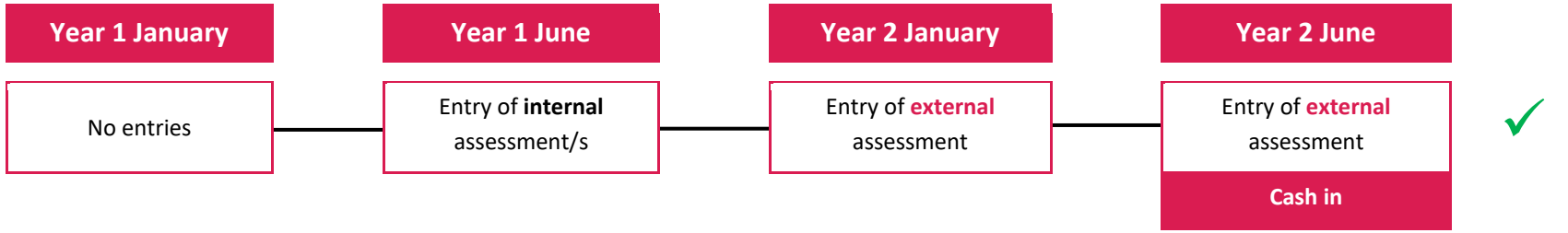
© WJEC CBAC Ltd.

Scenario 2:



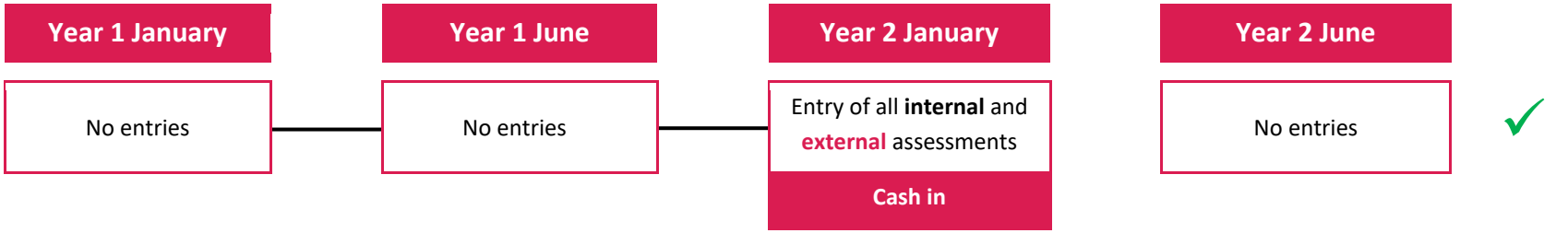
Entry for external assessment **does not** take place in the same series as cash-in and certification.

Scenario 3:



It is the **second** attempt of the external assessment that will count towards the final grade, even if it is lower than the previous attempt.

Scenario 4:



This is a linear approach and would be permissible if the qualification was completed in either January or in June.

© WJEC CBAC Ltd.

Assessment of Unit 1

Unit 1: ICT in
On-screen examination: 1 hour 20 minutes
40% of qualification
80 marks: 120 UMS

An assessment (taken on-screen), comprising of a range of question types to assess specification content related to ideas and concepts in how IT can be used to fulfil the needs of organisations and individuals, how data and information is used and transferred, and legal, moral, ethical, cultural and environmental impacts of IT and the need for cybersecurity.

All questions are compulsory.

The assessment objective weightings for Unit 1 are:

AO1	AO2	AO3
20%	15%	5%

FAQs:

Can learners resit the Unit 1 assessment?

Candidates may resit the **externally** assessed unit, prior to certification; however, this qualification has a 40% terminal requirement which must be satisfied by the externally assessed unit. Therefore, only the uniform mark score from the attempt made in the series in which the candidate is cashing in the qualification will be used in calculating the final overall grade, even if this is lower than the previous attempt.

Candidates who are unhappy with the grade awarded for the qualification may choose to resit one or more units following certification.

Where the candidate resits the externally assessed unit, only the uniform mark score from the resit attempt will be used in calculating the final overall grade, even if this is lower than the previous attempt. The candidate does not need to resit the internally assessed unit as marks for the internally assessed unit may be carried forward for the lifetime of the specification.

Is the assessment available on paper?

The assessment is available on-screen only. In the case of technical or other difficulties that might prevent a candidate from sitting the on-screen exam, centres should contact WJEC.

What is the entry code for this unit?

		Entry Code
Unit 1	External	5539U1
Cash in code		5539QA

© WJEC CBAC Ltd.

Is this assessment compulsory?

Yes.

When can candidates sit the Unit 1 assessment?

Assessment opportunities will be available in January and May/June each year, until the end of the life of this specification. January 2024 will be the first assessment opportunity for Unit 1. It should be noted that the Terminal Assessment Rule requires this examination to be completed at the end of the qualification, it may not be 'banked'.

Are candidates assessed on their spelling, punctuation and grammar in this assessment?

No, although learners are reminded of the need for good English and orderly, clear presentation in their answers.

Will candidates be expected to answer questions about content in Unit 2 in this exam?

No.

Will the assessment objective weightings remain the same throughout the life of the specification?

Yes.

How is the unit reported?

This unit will be graded Level 1 Pass, Level 1 Merit, Level 1 Distinction, Level 1 Distinction*, Level 2 Pass, Level 2 Merit, Level 2 Distinction, Level 2 Distinction*.

Will learners be expected to answer questions from across the whole specification?

No.

© WJEC CBAC Ltd.

GLOSSARY FOR UNIT 1

Term	Definition
Application software	A program containing a set of instructions to the computer that allows the user to carry out a specific function.
Artificial Intelligence (AI)	When computers perform tasks normally requiring human intelligence, such as problem solving, adapting according to previous experience.
Augmented reality	The process of superimposing a computer-generated image on a user's view of the real world.
Authentication	When a user confirms their unique identity on a computer system.
Back-up	A copy of a file that is kept in a location away from the computer which can be used to restore data in case of loss.
Biometrics	Technologies that recognise human body characteristics (e.g., fingerprint) to authenticate a person's identity.
Bionics	The science of constructing artificial systems (e.g., limbs) that have some of the characteristics of biological systems.
Bluetooth	A wireless communication protocol for exchanging data over short distances.
Cloud computing	Software applications and data that are stored online and used through the Internet.
Communication software	A program designed to pass information from one system to another.
Compression	Making files smaller by reducing the number of bits used to store the information.
Cookies	Cookies are text files containing small pieces of data that are sent from the website you are browsing. They are stored in your computer and provide a way to recognise you and keep track of your preferences.
Cyberbullying	Bullying using digital communication tools such as the Internet or mobile phones.
Data	A collection of text, numbers or symbols in a raw or unorganised form.
Data capture	The process of taking information from a document and converting it into data which a computer can read.
DDoS	A distributed denial-of-service attack, which is a malicious attempt to disrupt the operation of a service or network by flooding the target with fake traffic.
Digital footprint	The data left behind when you have made an interaction online.

© WJEC CBAC Ltd.

Term	Definition
Drone	A flying robot that can be remotely controlled.
E-commerce	Commercial transactions made electronically on the Internet.
Encoding	The process of converting data from one form to another.
Encryption	The process of scrambling data when it is being sent to protect it from unauthorised users, as they do not have an encryption key to decode it.
Ethernet	The most usual way of connecting computers together in a local area network (LAN).
E-waste	Electronic appliances such as mobile phones, computers, and televisions that are thrown away without the intention of re-use.
Expert system	A computer system that stores facts and can search these facts for information according to a set of rules, copying the decision-making ability of a human expert.
Extranet	An extranet is a controlled private network that is accessible to some authorised users outside of the organisation.
Green IT	Environmentally responsible and eco-friendly use of computers and their resources in order to reduce the carbon footprint.
Hacking	The gaining of unauthorised access to data in a computer system.
Hardware	The physical components of a computer.
Information	Data that has been processed, normally by a computer, to give it meaning.
Information handling software	The process of gathering, recording and presenting information in a way that is helpful to others (e.g., in a graph).
Input device	A piece of equipment that transfers data into a computer so it can be processed.
Internet	A public worldwide system of computer networks.
Intranet	A private operated network where data content and access is controlled. It is insulated from the global internet.

© WJEC CBAC Ltd.

Term	Definition
Key logging	The use of a computer program to record every keystroke made by a computer user without their knowledge and usually in order to gain fraudulent access to passwords and other confidential information.
Knowledge	When a person gains information such as facts, or the understanding of information such as how to solve problems.
Local Area Network (LAN)	A network that links computers that are geographically close enough together to be hard wired.
Logical protection	Software security controls put in place to manage access to computer systems (e.g., passwords).
Malware	Short for malicious software, it covers all software that is specifically designed to disrupt, damage or gain unauthorised access to a computer system.
Near-field Communication (NFC)	A set of communication protocols based on a radio frequency (RF) field, designed to exchange data between two electronic devices through a simple touch gesture.
Open source software	Software that is distributed with its source code so that anyone can inspect, modify or enhance it.
Output device	A piece of equipment that receives data from your computer once it has been processed (e.g., a monitor).
Packet sniffing	A computer program or computer hardware that can intercept and monitor network traffic.
Physical protection	Protecting equipment by physically preventing access to it.
Port	A docking point available for connection to peripherals such as input and output devices.
Protocol	A standard set of procedures that allow data to be transferred between electronic devices.
Radio-frequency Identification (RFID)	A technology to record the presence of an object using radio signals.
Ransomware	A type of malware that prevents you from using your computer or accessing certain files until you pay a ransom to the hacker.
Robotics	The use of robots to perform tasks done traditionally by humans.
Social engineering	When users are tricked into making security mistakes, so they give up confidential information.
Social network	An online service or site that allows people to communicate with friends on the Internet using a computer or mobile phone.

© WJEC CBAC Ltd.

Term	Definition
Software	The programs that tell a computer what to do.
Spyware	Software that enables a user to obtain information about your computer activities by transmitting data secretly from your hard drive.
Storage device	A piece of internal or external hardware used for saving, carrying and extracting data from a computer.
System software	A type of computer program that operates a computer's hardware and provides a platform to run application programs.
Teleworking	When you work at home, while communicating with your office using a wide area network (WAN).
Topology	The way in which computers are arranged in a network.
Trojan Horse	A type of malware that is usually disguised as legitimate software used by hackers trying to gain access to your computer system.
USB	An industry standard method of transferring data between a host device (e.g. a computer) and a peripheral device (e.g. a mouse). Stands for Universal Serial Bus.
Utility software	A program designed to help to analyse, configure, optimise or maintain a computer.
Validation	Checking input to make sure it meets a set of defined rules and is sensible in order to prevent errors.
Verification	Checking input to make sure that the data entered is identical to the original source in order to prevent errors.
Videoconference	An electronic meeting, allowing users to hold face-to-face meetings without having to be in the same place physically.
Virtual reality	A computer-generated simulation in which a person can interact within an artificial three-dimensional environment.
Virus	A piece of code which is capable of copying itself and is placed on your computer with the aim of damaging the system.
Wearable technologies	Smart electronic devices that are designed to be worn by the user and have sensors that collect data such as heart rate.
Wide Area Network (WAN)	A telecommunications network that extends over a large geographical area, connecting more than one Local Area Network (LAN).
Wireless	Uses a technology such as radio or microwaves to transmit signals rather than using wires or cables.
Worm	A computer program that replicates itself in order to spread malicious code throughout your system.

© WJEC CBAC Ltd.