Unit 1

Unit title	ICT in Society
Unit entry code	5539U1
GLH	48
Vocational Context	Jobs in ICT exist in a variety of contexts. However, there are key areas of knowledge that any ICT specialist will be required to know. This base knowledge allows them to provide the best service and advice possible for their clients and the industries they are working in.
Overview of unit	This unit 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.
Topics	1.1 How IT can be used to fulfil the needs of organisations[5] 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
Assessment	This unit is externally assessed through a written examination. *Duration:* 1 hour 20 minutes *Number of marks:* 80 *Format:* Questions requiring objective responses, short and extended answers, based around applied situations. Learners will be required to use stimulus material to respond to questions. This assessment contributes 40% to the overall qualification grade.

[5] 'Organisations' – Encompasses government, private, public and third sector organisations and industries.

1.1 How IT can be used to fulfil the needs of organisations and individuals	
In this topic learners will gain knowledge and understanding of the: 1.1.1 Functionality of different hardware devices 1.1.2 Functionality of different software 1.1.3 Services provided by IT	
Content	**Amplification**
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.
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.
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 • 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.

1.2 How data and information is used and transferred

In this topic learners will gain knowledge and understanding of:

1.2.1 Why data must be fit for purpose

1.2.2 How input data is checked for errors

1.2.3 How data transfers over different types of network

1.2.4 Different types of connectivity

Content	Amplification
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.
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.
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.

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.

1.3 Legal, moral, ethical, cultural and environmental impacts of IT and the need for cybersecurity

In this topic learners will gain knowledge and understanding of the following areas:

1.3.1 Risks to information held on computers
1.3.2 The impact of data loss, theft or manipulation on individuals and businesses
1.3.3 Methods used to protect information
1.3.4 How moral and ethical issues affect computer users
1.3.5 How legal issues protect computer users
1.3.6 The cultural, personal and environmental impact of ICT
1.3.7 How a digital footprint can impact computer users

Content	Amplification
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.
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.
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.
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.

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 • 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.
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.