OTHM LEVEL 3 FOUNDATION DIPLOMA IN INFORMATION TECHNOLOGY

Qualification Number: 603/7029/4

Specification | January 2021

TABLE OF CONTENTS

QUALIFICATION OBJECTIVES

The objective of the OTHM Level 3 Foundation Diploma in Information Technology is to equip learners with the skills and knowledge required to work in the IT sector or progress to further study.

The qualification is designed to ensure that each learner has an opportunity to build sector knowledge and learn current skills and practices in computer systems, networks, coding, website development, mobile communications, cyber security and social media for business.

QUALITY, STANDARDS AND RECOGNITIONS

OTHM Qualifications are approved and regulated by Ofqual (Office of Qualifications and Examinations Regulation). Visit the register of Regulated Qualifications.

OTHM has progression arrangement with several UK universities that acknowledges the ability of learners after studying relevant Level 3-7 qualifications to be considered for advanced entry into corresponding degree year/top-up and Master's/top-up programmes.

REGULATORY INFORMATION

Qualification Title	OTHM Level 3 Foundation Diploma in Information Technology
Ofqual Reference Number	603/7029/4
Regulation Start Date	14/01/2021
Operational Start Date	18/01/2021
Duration	1 Year
Total Credit Value	60
Total Qualification Time (TQT)	600 Hours
Guided Learning Hours (GLH)	240 Hours
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Overall Grading Type	Pass / Fail
Assessment Methods	Coursework
Language of Assessment	English

EQUIVALENCES

OTHM qualifications at Level 3 represent practical knowledge, skills, capabilities and competences that are assessed in academic terms as being equivalent to GCE AS/A Levels.

QUALIFICATION STRUCTURE

The OTHM Level 3 Foundation Diploma in Information Technology consists of 6 mandatory units for a combined total of 60 credits, 600 hours Total Qualification Time (TQT) and 240 Guided Learning Hours (GLH) for the completed qualification.

Unit Ref. No.	Unit Title	Credit	GLH	TQT
L/618/6090	Computer Systems	10	40	100
R/618/6091	Coding and Website Development	10	40	100
Y/618/6092	Networks	10	40	100
M/618/6096	Mobile Communications	10	40	100
T/618/6097	Cyber Security	10	40	100
A/618/6098	Social Media for Business	10	40	100

DEFINITIONS

Total Qualification Time (TQT) is the number of notional hours which represents an estimate of the total amount of time that could reasonably be expected to be required in order for a Learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of a qualification.

Total Qualification Time is comprised of the following two elements –

a) *the number of hours which an awarding organisation has assigned to a qualification for Guided Learning, and*
b) *an estimate of the number of hours a Learner will reasonably be likely to spend in preparation, study or any other form of participation in education or training, including assessment, which takes place as directed by – but, unlike Guided Learning, not under the Immediate Guidance or Supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training.*

(Ofqual 15/5775 September 2015)

Guided Learning Hours (GLH) is defined as the hours that a teacher, lecturer or other member of staff is available to provide immediate teaching support or supervision to a student working towards a qualification.

Credit value is defined as being the number of credits that may be awarded to a Learner for the successful achievement of the learning outcomes of a unit. One credit is equal to 10 hours of TQT.

ENTRY REQUIREMENTS

OTHM Level 3 qualifications can be offered to learners from age 16.

OTHM does not specify entry requirements for these qualifications. OTHM ensures that learners admitted to the programme have sufficient capability at the right level to undertake the learning and assessment.

OTHM centres must ensure learners are recruited with integrity onto appropriate qualifications that will meet their needs, enable and facilitate learning and achievement enable progression. The qualification is offered in English.

English requirements: If a learner is not from a majority English-speaking country must provide evidence of English language competency. For more information visit English Language Expectations page

PROGRESSIONS

Successful completion of the OTHM Level 3 Foundation Diploma for Information Technology provides learners with the opportunity for workplace and academic progressions to a wide range of relevant undergraduate programmes including OTHM Level 4 diplomas.
For more information visit University Progressions page www.othm.org.uk.

DELIVERY OF OTHM QUALIFICATIONS

OTHM do not specify the mode of delivery for its qualifications, therefore OTHM Centres are free to deliver this qualification using any mode of delivery that meets the needs of their

Learners. However, OTHM Centres should consider the learners' complete learning experience when designing the delivery of programmes.

OTHM Centres must ensure that the chosen mode of delivery does not unlawfully or unfairly discriminate, whether directly or indirectly, and that equality of opportunity is promoted. Where it is reasonable and practicable to do so, it will take steps to address identified inequalities or barriers that may arise.

Guided Learning Hours (GLH) which are listed in each unit gives the Centres the number of hours of teacher-supervised or direct study time likely to be required to teach that unit.

ASSESSMENT AND VERIFICATION

All units within this qualification are internally assessed by the centre and externally verified by OTHM. The qualifications are criterion referenced, based on the achievement of all the specified learning outcomes.

To achieve a 'pass' for a unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Judgement that the learners have successfully fulfilled the assessment criteria is made by the Assessor.
The Assessor should provide an audit trail showing how the judgement of the learners' overall achievement has been arrived at.

Specific assessment guidance and relevant marking criteria for each unit are made available in the Assignment Brief document. These are made available to centres immediately after registration of one or more learners.

OPPORTUNITIES FOR LEARNERS TO PASS

Centres are responsible for managing learners who have not achieved a Pass for the qualification having completed the assessment. However, OTHM expects at a minimum, that centres must have in place a clear feedback mechanism to learners by which they can effectively retrain the learner in all the areas required before re-assessing the learner.

RECOGNITION OF PRIOR LEARNING AND ACHIEVEMENT

Recognition of Prior Learning (RPL) is a method of assessment that considers whether learners can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess and do not need to develop through a course of learning.

RPL policies and procedures have been developed over time, which has led to the use of a number of terms to describe the process. Among the most common are:

- Accreditation of Prior Learning (APL)
- Accreditation of Prior Experiential Learning (APEL)
- Accreditation of Prior Achievement (APA)
- Accreditation of Prior Learning and Achievement (APLA)

All evidence must be evaluated with reference to the stipulated learning outcomes and assessment criteria against the respective unit(s). The assessor must be satisfied that the

evidence produced by the learner meets the assessment standard established by the learning outcome and its related assessment criteria at that particular level.

Most often RPL will be used for units. It is not acceptable to claim for an entire qualification through RPL. Where evidence is assessed to be only sufficient to cover one or more learning outcomes, or to partly meet the need of a learning outcome, then additional assessment methods should be used to generate sufficient evidence to be able to award the learning outcome(s) for the whole unit. This may include a combination of units where applicable.

EQUALITY AND DIVERSITY

OTHM provides equality and diversity training to staff and consultants. This makes clear that staff and consultants must comply with the requirements of the Equality Act 2010, and all other related equality and diversity legislation, in relation to our qualifications.

We develop and revise our qualifications to avoid, where possible, any feature that might disadvantage learners because of their age, disability, gender, pregnancy or maternity, race, religion or belief, and sexual orientation.

If a specific qualification requires a feature that might disadvantage a particular group (e.g. a legal requirement regarding health and safety in the workplace), we will clarify this explicitly in the qualification specification.

UNIT SPECIFICATIONS

Computer Systems

Unit Reference Number	L/618/6090
Unit Title	Computer Systems
Unit Level	3
Number of Credits	10
Total Qualification Time (TQT)	100
Guided Learning Hours (GLH)	40
Mandatory / Optional	Mandatory
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Unit Grading Structure	Pass / Fail

Unit Aims

The aim of this unit is to introduce learners to the basic hardware and software components that make up computer systems and for learners to carry out basic installation and configuration. This unit is designed to assist learners to understand the basic components of computer systems and how they are adapted to individual needs.

Learning Outcomes, Assessment Criteria and Indicative Content

Learning Outcomes – The learner will:	Assessment Criteria – The learner can:	Indicative contents
1. Understand the purpose of computer systems.	1.1 Explain different types of computer systems. 1.2 Evaluate the role of computer systems in different environments. 1.3 Identify a range of computer systems that you use.	• **Computer system:** types Personal Computer (PC), laptop, netbook, smartphone, smartwatch, games consoles, tablet, server, IoTs • **Environment:** Manufacturing, production, home, office, education, medical, pharmaceutical, retail, sports etc. • **Personal use**
2. Understand computer system components.	2.1 Discuss the common Hardware components of a computer system 2.2 Discuss the common Software components of a	• **Hardware components:** The Arithmetic and Logic Unit; ALU, Control Unit and Registers (Program Counter; PC, Accumulator; ACC,

	computer system 2.3 Evaluate the differences between open source and closed source software.	Memory Address Register; MAR, Memory Data Register; MDR, Current Instruction Register; CIR). Storage devices: hard disk drive, ROM, flash drive, DVD/ Blu-ray Disc (BD). Input devices: touch screen, graphics tablet, gaming controller, microphone, mouse, keyboard. Output devices: printer, monitor, sound. Computer network connectivity: 3G, Wireless, Bluetooth, NIC. • **Software components:** System software, Applications software, Software utilities. • **Open source vs closed source** Pricing, availability, scope of engagement, structures, codes, platforms.
3. Be able to configure computer systems.	3.1 Analyse different operating systems and their suitability in managing resources in a professional environment. 3.2 Describe the characteristics of different styles of computer system users. 3.3 Evaluate suitable components to meet user requirements within a professional environment. 3.4 Configure a computer system for a given user requirement.	• **Operating systems:** Microsoft Windows (like Windows 10, Windows 8, Windows 7, Windows Vista, and Windows XP), Apple's macOS (formerly OS X), Chrome OS, Linux, Unix, Ubuntu etc. • **System users:** describe the characteristics of different styles of user interface, command-based, forms, dialogue, natural language, wimp interfaces (windows, icons, menus, pointer), and their appropriate uses. • **Requirements:** users eg office, home; tasks eg data recording, photo/video editing, media. • Home, Business, Networking, Real-time, Communication. **Systems software:** eg operating systems, systems software tools, diagnostic tools, file managers, disk utilities, back up, synchronisation; network connections eg workgroups, email, ftp. **Applications software**: office applications

		software eg word processing, spreadsheet, presentation, database, graphics, web browser, email client **Utilities:** clean up tools eg for cookies, internet history, defragmentation; drive formatting; antivirus, adblocker **Connect and set up:** equipment eg monitor, printer, modem/router, keyboard, mouse, speakers, microphone, RAM, hard drive Install hardware: components eg graphics card, sound card, CD/DVD drive Install software: operating system software eg Windows; applications software eg Microsoft Office; security software eg virus checkers, firewalls; device drivers; create appropriate directory/folder structures; other devices eg tablets / phones use other operating systems.

Assessment

To achieve a 'pass' for this unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Learning Outcomes to be met	Assessment criteria to be covered	Type of assessment	Word count (approx. length)
All 1 to 3	All AC under LO 1 to 3	Coursework	3000 words

Indicative Reading list

- Nisan, N. (2020). *The Elements of Computing Systems : building a modern computer from first principles.* MIT Press.
- Bryant, R.E. and O'Hallaron, D.R. (2016). *Computer systems : a programmer's perspective*. Boston: Pearson.

Coding and Website Development

Unit Reference Number	R/618/6091
Unit Title	Coding and Website Development
Unit Level	3
Number of Credits	10
Total Qualification Time (TQT)	100
Guided Learning Hours (GLH)	40
Mandatory / Optional	Mandatory
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Unit Grading Structure	Pass / Fail

Unit Aims

The aim of this unit is to enable learners to understand the fundamental processes involved in developing simple programmes and applications, as well as details of basic website design.

Learning Outcomes, Assessment Criteria and Indicative Content

Learning Outcomes – The learner will:	Assessment Criteria – The learner can:	Indicative contents
1. Understand the purpose and types of coding.	1.1 Identify popular programming languages that are used within computer systems. 1.2 Differentiate between High level and Low-level programming languages. 1.3 Explain how principles of computer programming are applied in different languages to produce software applications.	• The uses and applications of different types of high and low-level programming languages, developed to assist in the solution of particular problems, such as: o procedural, e.g. C, Perl®, PythonTM o object-orientated, e.g. C++, C#®, Java® o event-driven, e.g. Visual Basic® o machine, e.g. Assembler o mark-up, e.g. HTML. • Factors to compare and contrast in programming languages, including: o hardware and software needed for running

		and developing a program ○ special devices required ○ performance ○ preferred application areas ○ development time ○ ease of development.
2. Understand web architecture and components.	2.1 Explain the web architecture and components which enable internet and web functionality 2.2 Discuss the security risks and protection mechanisms involved in website performance.	• Web architecture: Internet Service Providers (ISP); web hosting services; domain structure; domain name registrars; worldwide web • Components: hardware eg web, mail and proxy servers; routers; software eg browser, email • Protocols: transport and addressing eg TCP/IP; application layer eg HTTP, HTTPS, SMTP • Web functionality: Web 1.0, Web 2.0; blogs; online applications; cloud computing • Security: risks eg hacking, viruses, identity theft Security protection mechanisms: firewalls; • Secure Socket Layers (SSL); adherence to standards eg strong passwords
3. Be able to create interactive websites.	3.1 Be able to create or modify components of websites to meet business needs. 3.2 Demonstrate that a created website meets the defined requirements and achieves the defined purpose.	• **Design:** • select appropriate software e.g. standard and non-standard • use formatting and editing techniques, e.g.: ○ common web functions (e.g. text, graphics, fonts, text formatting, colour schemes, images) ○ simple HTML (e.g. editor programs, file extensions) ○ HTML tags and conventions (e.g. <html>, <p>, <body>, closing tags) • introduce interactive elements (e.g. rollover images, submit button to email a form) • apply optimisation (e.g. image, video, animation, sound, file, size, format, dimensions,

		compression)
		• apply good practice, i.e.:
		  o consistent file and folder management
		  o appropriate naming conventions
		  o documentation of developments
		• ensure accessibility, i.e.users with disabilities (e.g. accessibility aids, readability, colour scheme, subtitles)
		• **Plan and present the solution:**
		  o format of presentation
		  o content of presentation
		  o target audience
		  o obtain feedback from audience
		• **Recommend changes to website components:**
		  o appropriateness
		  o clarity
		  o content
		  o speed
		  o navigation
		  o aesthetics
		• **Comparison of website components against business needs:**
		  o comparison of updated website against business needs
		  o demonstration of functionality
		  o demonstration of interactivity
		  o present the solution to the stakeholders
		Review website components:
		• feedback, e.g.:
		  o questionnaires
		  o verbal discussion
		• identify criteria for feedback e.g. appropriateness, clarity, content, speeds, navigation, font choice, colour

		combinations)analysis • improvements (e.g. design, clarity, interactive response, function)

Assessment

To achieve a 'pass' for this unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Learning Outcomes to be met	Assessment criteria to be covered	Type of assessment	Word count (approx. length)
All 1 to 3	All AC under LO 1 to 3	Coursework	3000 words

Indicative Reading list

- Bell, A. (2019). *Computer programming : Fundamentals for absolute beginners*.
- Duckett, J. (2011). *HTML & CSS: Design and Build Websites (HTML and CSS)*. John Wiley & Sons Incorporated.
- Felleisen, M. et al (2018) *How to design programs: an introduction to programming and computing.* 2nd ed. MIT Press
- Robbins, J.N. (2018). *Learning web design : a beginner's guide to HTML, CSS, Javascript, and web graphics*. Sebastopol, Ca: O'Reilly.

Networks

Unit Reference Number	Y/618/6092
Unit Title	Networks
Unit Level	3
Number of Credits	10
Total Qualification Time (TQT)	100
Guided Learning Hours (GLH)	40
Mandatory / Optional	Mandatory
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Unit Grading Structure	Pass / Fail

Unit Aims

The aim of this unit is to enable learners to understand the importance of networks to computer systems and their essential use in a variety of application. Learners will also gain knowledge about network technologies and the delivery of a wide range of networked services.

Learning Outcomes, Assessment Criteria and Indicative Content

Learning Outcomes – The learner will:	Assessment Criteria – The learner can:	Indicative contents

1. Understand networking principles .	1.1 Explain a computer network.
	1.2 Differentiate between 'client computers' and 'peer computers' from network services perspective.
	1.3 Describe local area network (LAN) and wide area network (WAN).
	1.4 Describe the benefits and constraints of different network topologies.
		• Computer Network:
		  ○ sharing hardware resources
		  ○ sharing software resources
		  ○ sharing common data
		  ○ potential intranet provision
		  ○ e-mail communication between users
		  ○ centralised management services
		• 'Client computers' and 'Peer computers'
		• LAN and WAN including VLAN, WLAN and VPN
		• Topology:
		  ○ Linear Bus Topology
		  ○ Ring Topology

		○ Star Topology ○ Mesh Topology ○ Tree Topology ○ Hybrid Topology
2. Understand how network hardware and software components are connected.	2.1 Explain how hardware, software and addressing combine to support network communications. 2.2 Describe potential issues with computer networks. 2.3 Explain the steps required to set up and test a simple local area network.	• **Hardware:** network cards eg ethernet, wireless; workstations; servers eg file, printer, web; routers; switches; wireless devices • **Communication:** network cabling eg fibre optics, UTP, STP, coaxial; connectors; addressing; WAN connectivity eg ADSL, ISDN, broadband • **Software:** application-based eg internet browsers, firewalls, email; operating system; utility • **Issues:** speed eg bandwidth, contention; costs; staff skills; down time; security issues eg unauthorised access, loss of data, malware, virus protection; backup eg recovery; hacking; firewalls **Setup:** • Preparation: components eg cabling, devices, network interface cards, software • Set up: hardware; software; security; health and safety awareness • Simple LAN: eg peer to peer, client-server • Faults: commonly occurring eg address conflict, network card failure, faulty cable; loss of service eg print, file, email • Testing: functionality; connectivity; addressing • Security: eg firewall configuration, file and folder permissions, access control, user rights • Use: communication; transfer files; others eg allocate user rights, allocate file space

		• Troubleshoot: problem solving eg connectivity, IP addresses
3. Understand the usage and security concerns related to networking.	3.1 Evaluate the features and services provided by a local and a wide area network. 3.2 Identify security issues related to networking and how those security issues can be minimised. 3.3 Explain steps to configure security on a local area network.	• Features: topologies eg star, bus, circle; types eg peer-to-peer, client server; data rates; addressing eg IP, MAC Services: communication eg email, conferencing; file transfer; login; security; software deployment • Security: eg firewall configuration, file and folder permissions, access control, user rights • Wireless encryption methods: WPA, WPA2, WEP, Dynamic Host Configuration Protocol (DHCP), Remote Access

Assessment

To achieve a 'pass' for this unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Learning Outcomes to be met	Assessment criteria to be covered	Type of assessment	Word count (approx. length)
All 1 to 3	All AC under LO 1 to 3	Coursework	3000 words

Indicative Reading list

- Kurose, J. & Ross, K. (2017) *Computer Networking: a top-down approach*. 7th ed. Pearson
- Kizza, J. (2015) *Guide to Computer Network Security*. 3rd ed. Springer
- Tanenbaum, A. & Wetherall, D. (2013) *Computer Networks*. 5th ed. Pearson

Mobile Communications

Unit Reference Number	M/618/6096
Unit Title	Mobile Communications
Unit Level	3
Number of Credits	10
Total Qualification Time (TQT)	100
Guided Learning Hours (GLH)	40
Mandatory / Optional	Mandatory
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Unit Grading Structure	Pass / Fail

Unit Aims

The aim of this unit is to explain the growth of mobile communication and how it has changed everyday life and to provide learners with an understanding of the functionality that underpins key business and e-commerce uses.

Learning Outcomes, Assessment Criteria and Indicative Content

Learning Outcomes – The learner will:	Assessment Criteria – The learner can:	Indicative contents
1. Understand the uses and features of mobile communication devices.	1.1 Differentiate between different types of mobile communication device 1.2 Describe the main features of different types of mobile communication devices 1.3 Evaluate usage of modern mobile communication devices.	• **Devices**: types eg mobile phones, digital cordless phones, PDAs, laptops, palmtops; other eg radio frequency identification devices (RFID) • **Features**: eg video link, texting, internet access, email, picture messaging, GPS tracking, geocaching, synchronisation, cloud storage • **Uses:** business eg email, word processing, conferencing, calendar; specialist eg graphic design, bespoke software, monetary transactions, service management; personal eg online gaming, messaging, web browsing.

2. Understand the communication technologies used in mobile devices.	2.1 Discuss various transmission technologies used by mobile communication devices. 2.2 Evaluate the need for various standards and protocols used by mobile communication devices. 2.3 Describe how wireless mobile communication technologies are benefitting businesses.	• **Transmission technology:** types eg infrared, Bluetooth, Wireless Fidelity (WiFi), GSM, GPRS, 2.5G, 3G; data transfer rates; effective ranges Standards and protocols: types eg 802.11 for WiFi, IrDA for Infrared; wireless access protocols; SMS protocols . • **Wireless networking**: wireless access points eg hotspots; wireless network adaptors; Protection: methods eg wireless encryption methods (WEP, WPA, AES, EAP); interference from other devices. Communication eg email, conferencing; file transfer.
3. Understand the implications of mobile communications technology.	3.1 Assess the benefits of mobile devices in workplace. 3.2 Evaluate social and legal implications of using mobile technologies. 3.3 Discuss the health implications of long exposer to mobile technologies.	• **Benefits**: efficiency eg group communication, information sharing, paperless working • **Social implications**: human interaction eg text messaging, multimedia messaging, emails, virtual offices; • **Health issues** eg posture, RSI, eye strain; environmental effects eg visual impact of phone masts, disposal of components; illegal imagery • **Legal implications:** data security eg accidental loss, theft; hacking activities eg wardriving, piggybacking, packet sniffing; • **Disadvantages:** effective range of equipment; interference; perceived health hazards eg radiation

Assessment

To achieve a ‘pass’ for this unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Learning Outcomes to be met	Assessment criteria to be covered	Type of assessment	Word count (approx. length)
All 1 to 3	All AC under LO 1 to 3	Coursework	3000 words

Indicative Reading list

- Greengard, S. (2015) *The Internet of Things*. MIT Press
- Shah, M. (2014) *Mobile Working: technologies and business strategies*. Routledge
- Rowles, D. (2014) *Mobile Marketing: how mobile technology is revolutionizing marketing, Communications and advertising*. Kogan Page

Cyber Security

Unit Reference Number	T/618/6097
Unit Title	Cyber Security
Unit Level	3
Number of Credits	10
Total Qualification Time (TQT)	100
Guided Learning Hours (GLH)	40
Mandatory / Optional	Mandatory
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Unit Grading Structure	Pass / Fail

Unit Aims

The aim of this unit is to enable learners to understand about cyber security and the consequences and implications of inadequate cyber security. They will understand key terminology and the motivations of good and bad actors. They will also investigate the advantages and disadvantages of security by design.

Learning Outcomes, Assessment Criteria and Indicative Content

Learning Outcomes – The learner will:	Assessment Criteria – The learner can:	Indicative contents
1. Understand cyber security.	1.1 Describe the concepts of cyber security. 1.2 Explain the importance of cyber security for businesses. 1.3 Describe the consequences and implications of inadequate cyber security for businesses .	• **Concepts of cyber security:** security, identity, confidentiality, integrity, availability, threat, vulnerability, risk, hazard. • **Importance of cyber security:** cost of breaches, sophisticated hackers, widely available hacking tools, tighter regulations (GDPR) • **Consequences and implications:**

		unauthorised access to distribution of or loss of, sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, industry information systems.
2. Understand core terminology and key aspects of cyber security.	2.1 Define core terminology used in cyber security. 2.2 Compare typical behaviours of good actors and bad actors. 2.3 Discuss key sectors that are most vulnerable to a cyber-attack.	• **Core terminology:** malicious software, distributed denial of service (DDoS), cloud , software, domain , exploit, breach, firewall, encryption, Virtual Private Network (VPN), IP address, malware, virus, social engineering Bring Your Own Device (BYOD, Penetration testing (pen testing):process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. o white-box penetration test is to simulate a malicious insider who has knowledge of and possibly basic credentials for the target system. o black-box penetration test is to simulate an external hacking or cyber warfare attack. • **Good and bad actors:** o **bad** – ex employee, black hat, script kiddies, hacktivist, organised crime hackers, o **good** – white hat, certified penetration tester. • **Key sectors:** manufacturing, finance, government and defence agencies/departments, educational institutions, utilities, maritime, IT, healthcare, retailers,
3. Understand cyber threat intelligence.	3.1 Identify key concepts of cyber threat intelligence 3.2 Explain the following terms in relation to cyber security: • threats • exploits • vulnerabilities	• Cyber threat intelligence - information an organisation uses to understand the threats that have, will, or are currently targeting the organisation ie sources: open source intelligence, social media intelligence, human Intelligence, technical intelligence or deep and

	• risks 3.3 Identify improvements to secure a network against cyber attacks.	dark web intelligence • **Terminologies:** • **Threats** - an agent that may want to or definitely can result in harm to the target organisation ie employee sabotage and theft, including of physical equipment or data, and damage such as fire, flood, power loss, terrorism or other disaster o unauthorised access by employees and other users to secure areas and administration functions, including security levels and protocols o weak cyber security measures and unsafe practices, including security of computer equipment and storage devices, security vetting of visitors, visiting untrustworthy websites, accidental loss or disclosure of data, including poor staff training and monitoring, malicious software (malware), including spyware, adware, ransomware; viruses, including worms, rootkits and trojans o hacking, including commercial, government, individuals, sabotage, including commercial, government, terrorism, individuals o social-engineering techniques used to obtain secure information by deception. • **Exploits** - code that takes advantage of a software vulnerability or security flaw. o A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system. o A local exploit requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator. Exploits against client applications also exist, usually

		consisting of modified servers that send an exploit if accessed with a client application. • **Vulnerability** – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorised access to an asset ie could include but not limited to network, including firewall ports and external storage devices o organisational, including file permissions or privileges, password policy, software, including from an untrustworthy source, downloaded software, illegal copies, SQL injection and new zero-day exploits, operating system, including unsupported versions, updates not installed on mobile devices, reliant on Original Equipment Manufacturers (OEMs) to update system software, physical including theft of equipment, Universal Serial Bus (USB) storage devices with sensitive data, collection of passwords and other information by social-engineering methods o process of how people use the system, including leaks and sharing security details, security implications of cloud computing and of the Internet of Things (IoT) devices • **Risk**s is where threat and vulnerability may overlap ie could include but are not limited to social engineering (art of manipulating people so they give up confidential information) phishing, blagging (pretexting), phishing, pharming, shouldering (or shoulder surfing), ransomware , Denial of Service (DoS)/Distributed Denial of Service (DDoS), virus. • **Secure Network:** biometric measures (particularly for mobile devices), password systems, CAPTCHA (or

		similar), using email confirmations to confirm a user's identity, automatic software updates.

Assessment

To achieve a 'pass' for this unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Learning Outcomes to be met	Assessment criteria to be covered	Type of assessment	Word count (approx. length)
All 1 to 3	All AC under LO 1 to 3	Coursework	3000 words

Indicative Reading list

- Easttom, C. (2016) *Computer Security Fundamentals*. 3rd ed. Pearson
- Kizza, J. (2015) *Guide to Computer Network Security*. 3rd ed. Springer
- Geetha, S. & Phamila, A. (2016) *Combating Security Breaches and Criminal Activity in the Digital Sphere*. Hershey

Social Media for Business

Unit Reference Number	A/618/6098
Unit Title	Social Media for Business
Unit Level	3
Number of Credits	10
Total Qualification Time (TQT)	100
Guided Learning Hours (GLH)	40
Mandatory / Optional	Mandatory
Sector Subject Area (SSA)	14.1 Foundations for learning and life
Unit Grading Structure	Pass / Fail

Unit Aims

The aim of this unit is to allow learners to explore how businesses use social media to promote their products and services. Learners will also create a social media policy and plan to meet business requirements.

Learning Outcomes, Assessment Criteria and Indicative Content

Learning Outcomes – The learner will:	Assessment Criteria – The learner can:	Indicative contents
1. Understand the importance of using social media in a business environment.	1.1 Discuss recent developments in social media that have changed the way businesses promote products and services. 1.2 Identify sources for social media channels to meet business needs. 1.3 State the importance of publishing social media content which engages the audience. 1.4 Explain the risks and issues related to social media engagement.	• **Features of social media:** advertising, e-commerce, search engine optimization (SEO), Facebook Insights, Twitter Analytics and Google Analytics, Instagram, Audience profiles (age, gender, income) of social media websites. • **Business Needs:** • Creating an image or brand, promoting products and/or services, resolving queries and managing issues. • Aims and objectives, eg control publishing, control marketing, advertise to wider

		audiences, build online business, open up business opportunities, develop/establish a brand, help grow a business, connect to wider/global markets, connect with new groups/types of customer, establish a reputation, improve internal communication, generate leads/sales, improve staff recruitment/retention, improve customer support/satisfaction, save money • Emergence of influencers, eg: online, eg tweeters, bloggers, e-zine authors, offline, eg politicians, journalists, TV personalities, objects, eg photos, videos, music, tweets, blogposts, speeches, organisations, eg pressure groups, lobbyists, consumer organisations • **Types of content:** eg images, video, audio, text, links, polls, quizzes. Types of audience: eg general public, niche, existing customers, internal. Matching content to audience • **Issues:** o growth in popularity o attitudes of different cultures and population sectors o accessibility o legislation covering use o cyber bullying o health issues o unforeseen consequences of posted content and damage to reputation. o data protection and data handling considerations o ethical considerations

		○ Risks, eg malware, legal liability for posted content, time wasting, vulnerability to hackers, vulnerability to malicious posters/commenters, disclosure of confidential information.
2. Understand the need for social media content planning and publishing in a business environment.	2.1 Discuss considerations for regular posts and other content to be published on social media websites. 2.2 Explain the relationship between a social media website and company website. 2.3 Evaluate strategy required to create and encourage an online community.	• **Engagement considerations:** identifying a target audience (e.g. age, gender, interests, income) • linking type of content to target audience to ensure it is engaging. • **Relationship between social media website and company website**, e.g. using: social media buttons on the company website, company website links within social media posts that encourage visits to e-commerce site to make purchases, social media news feeds on the company website. • **Strategy:** use of promotional techniques, e.g. requesting feedback, surveys, special offers and creating links between social media websites and company e-commerce site • monitoring social media website streams and responding to queries, requests and complaints. • I**mplementation of an online community**: building strategy, including: use of hashtags, sharing and tagging, finding and joining groups and contributing information, following people and businesses.
3. Be able to develop a policy and a plan to use social media in a business environment.	3.1 Explain why a social media policy is important and consider the implications of not having a policy in place. 3.2 Develop a social media policy for a business. 3.3 Produce a plan to use social media in a business environment.	**Specific business requirements:** ○ Content planning and publishing ○ Developing online communities ○ Enforcing social media policies. ○ Company philosophy (identifying and reflecting this in posted content)

	3.4 Produce a reflective account of the plan to suggest improvements.	○ Promotion of honesty and respect in posted content ○ Ways to ensure confidentiality of information ○ Methods of dealing with security issues ○ Separation of company and personal content ○ Relevant legal and ethical considerations • Consequences of not having a policy, eg legal liability, public relations problems, potential conflict between employees and employers/industrial relation problems, time wasting **Plan:** ○ process of planning posts and other content to be published on social media websites ○ identifying a target audience (e.g. age, gender, interests, income, location) ○ linking type of content to target audience to ensure it is engaging ○ researching keywords and creating keyword strategies to help users identify content ○ researching the best time to publish content and creating a publishing schedule ○ concept of working with a client to develop a strategy to encourage online community building, including: use of promotional techniques, e.g. requesting feedback, surveys, special offers and creating links between social media

		websites and company e-commerce site ○ monitoring social media website streams and responding to queries, requests and complaints. **Reviewing and refining plans:** ○ implications of working with a client to improve the quality, ○ effectiveness and appropriateness of the plans. ○ gathering feedback from a client and potential users, communicating with a client, e.g. email, verbal communication, ○ scheduling and documenting meeting, ○ agreeing and adjusting timescales, ○ refining ideas and solutions.

Assessment

To achieve a 'pass' for this unit, learners must provide evidence to demonstrate that they have fulfilled all the learning outcomes and meet the standards specified by all assessment criteria.

Learning Outcomes to be met	Assessment criteria to be covered	Type of assessment	Word count (approx. length)
All 1 to 3	All AC under LO 1 to 3	Coursework	3000 words

Indicative Reading list

- Lipschultz, J. (2015) *Social media Communication: concepts, practices, data, law and ethics*. Routledge
- Kasian-Lew, D. (2014) *The Social Executive: why leaders need social media and why it's good for business.* Wiley-Blackwell

IMPORTANT NOTE

Whilst we make every effort to keep the information contained in programme specification up to date, some changes to procedures, regulations, fees matter, timetables, etc may occur during the course of your studies. You should, therefore, recognise that this booklet serves only as a useful guide to your learning experience. For updated information please visit our website www.othm.org.uk.