eduqas

LEVEL 2 FOUNDATION CERTIFICATE

Digital Systems and Data

First teaching from September 2027, First Award 2029

Draft Specification

This DRAFT specification has yet to be approved by Ofqual. Centres should therefore expect changes in the final approved version.

Behind *every* TEACHER

Qualification title	WJEC Level 2 Foundation Certificate in Digital Systems and Data
Qualification objective	The WJEC Foundation Certificate in Digital Systems and Data provides learners with the knowledge, understanding and skills associated with a broad vocational area. The qualification supports progression to Level 3 academic, technical and vocational study while providing an engaging programme of applied learning. Achievement in the qualification provides valid and reliable evidence of attainment that may be used to support progression decisions by education and training providers. It is designed to prepare learners for successful progression to further study and training within the vocational area.
WJEC Qualification Code	
QAN Number	
Age groups approved for	16–19, 19+
First teaching	September 2027
First certification	Summer 2028

Version	Description	Date
Our specifications may change over time. WJEC will inform centres of any amendments and the most up to date version of the specification will always be on the website.		

Supporting Qualification Documents

This specification provides the depth and breadth of the teaching and learning content, you should also refer to the other qualification-specific documents available on our website, including:

- Assessment Administration Guide
- Sample Assessment Materials; including
  - Candidate Assessment Packs
  - Information for teachers
  - Candidate brief
  - Mark scheme
  - Resource files.

© WJEC CBAC Ltd 2027.

This specification meets the requirements of the following regulatory documents published by Ofqual:

- Foundation Certificate Qualification Level Conditions and Requirements, which set out the regulatory requirements that apply to all Foundation Certificate qualifications.
- Foundation Certificate Qualification Level Guidance, which supports compliance with the Foundation Certificate Qualification Level Conditions and Requirements.
- Foundation Certificate Level Conditions and Requirements for Digital Systems and Data, which set out the additional requirements specific to this Foundation Certificate subject.
- General Conditions of Recognition, which contain the rules that all awarding organisations and their qualifications must meet when offering regulated qualifications in England.

DRAFT

© WJEC CBAC Ltd 2027.

Learning and achieving together

Educational reform creates opportunities for innovation and improvement, but it also brings significant demands for schools and colleges. Successfully introducing new qualifications requires more than effective qualification design; it requires an awarding organisation with the experience, expertise and commitment to support centres every step of the way.

WJEC has extensive experience developing and delivering both general and vocational qualifications and supporting centres through periods of qualification reform. Through close collaboration with teachers, leaders, employers and industry specialists, we understand the realities of implementing change and the practical support needed to ensure successful delivery.

Our approach is built on partnership. We recognise that introducing a new qualification is a significant investment of time, resource and expertise, and we are committed to working alongside centres from first approval through to first assessment and beyond. We listen to feedback, respond to emerging needs and continually refine our support to ensure it remains relevant, practical and effective.

Centres choosing WJEC will have access to a comprehensive support package designed to build confidence and reduce workload. This will include high-quality teaching and learning resources, detailed qualification guidance, assessment support materials, exemplification, professional learning opportunities, regular communications and access to subject specialists. Our support package will help centres understand qualification requirements, prepare learners effectively and approach assessment with confidence.

We believe that successful qualifications are built on strong relationships. By combining subject expertise, responsive support and a deep understanding of educational change, we aim to provide centres with the confidence to embrace new opportunities and focus on what matters most: delivering outstanding outcomes for learners.

As Foundation Certificates are introduced, our commitment is to be a trusted partner for centres, providing the guidance, resources and expertise needed to support successful implementation and long-term delivery.

DRAFT

© WJEC CBAC Ltd 2027.

Contents

Summary of assessment 6
1. Introduction 7
1.1. Purpose and aims 7
1.2. Prior learning and progression 8
1.3. Guided Learning Hours (GLH) and Total Qualification Time (TQT) 9
1.4. Use of language 9
1.5. Equality and fair access 10
2. Content areas 11
2.1. Content area format 11
2.2. How to read the amplification 11
2.3. Teaching content 11
Content Area 1: Foundations of Digital Systems and Data 12
Content Area 2: Digital Data and Sources in Practice 40
Content Area 3: Digital Systems in Practice 48
3. Assessment 57
3.1. Assessment overview 57
3.2. Synoptic assessment 58
4. Technical information 59
4.1. Assessment availability 59
4.2. Assessment entries 59
4.3. Claiming the qualification 59
4.4. Assessment reporting 59
Appendix A – Glossary of terms 61
Appendix B – Minimum delivery requirements/resources 68
Appendix C – Transferable skills 70
Appendix D – Mapping to Level 3 qualifications 72

Copyright
© WJEC CBAC Limited, 2027.

WJEC operates in England under the trading name Eduqas. WJEC CBAC Ltd is a registered company (03150875) and registered charity (1073332).

Summary of assessment

This qualification has five learning outcomes and each is divided into 'knowledge and understanding' (KU) and 'skills' (SK) content.

- Knowledge and understanding – the theoretical facts, principles, concepts, and procedures that learners should acquire.
- Skills – the subject-specific and transferable skills needed to achieve a learning outcome.

LO1	Clean, interpret and visualise a dataset in order to answer a question and communicate findings clearly
LO2	Configure and secure digital systems by applying access, authentication and configuration measures
LO3	Plan, develop and test a programming solution in order to meet a brief
LO4	Plan and configure hardware and software components in order to deliver a functional digital system
LO5	Select and apply reliable digital sources to produce evidence-based recommendations for an intended purpose

Content Area	Assessment	Weighting	Marks/Points
Content Area 1: Foundations of Digital Systems and Data LO1–5KU	**Assessment 1:** Assessment by examination: 1 hour 30 minutes	40% of qualification	80 marks
Content Area 2: Digital Data and Sources in Practice LO1SK+LO5SK	**Assessment 2:** Non-exam assessment: 7 hours	24% of qualification	36 marks
Content Area 3: Digital Systems in Practice LO2–LO4 SK	**Assessment 3:** Non-exam assessment: 15 hours	36% of qualification	63 marks

Click here to enter accreditation number.

© WJEC CBAC Ltd 2027.

1. Introduction

1.1. Purpose and aims

WJEC Foundation Certificates are designed for learners who wish to develop knowledge, understanding and skills within a broad vocational area and who may require further preparation before progressing to Level 3 study.

The qualifications engaging and applied learning experiences that combine the development of vocational knowledge with opportunities to apply learning in authentic contexts. Learners develop subject-specific knowledge and skills alongside transferable skills and work-related behaviours that support future learning.

Foundation Certificates are intended primarily to support progression to Level 3 qualifications across technical, vocational and academic pathways. They form part of a broader programme of study and may be undertaken alongside qualifications in English and mathematics.

Achievement in a Foundation Certificate provides reliable evidence that a learner has met the knowledge, understanding and skills requirements of the qualification and is ready to progress within the subject area.

WJEC Foundation Certificates:

- provide learners with nationally agreed knowledge, understanding and skills within a broad vocational area
- enable learners to apply their learning in practical and work-related contexts
- motivate learners and support progression to Level 3 study in a related subject area
- develop transferable skills and behaviours valued in further learning and employment
- provide valid and reliable evidence of learner attainment
- support schools, colleges and other providers in making progression decisions and demonstrating learner achievement

This qualification is aligned with Level 2 of the Regulated Qualifications Framework (RQF) and forms part of the Foundation Certificate qualification suite regulated by Ofqual.

The aims and purpose of the Foundation Certificate in Digital Systems and Data is to enable learners to:

- apply their knowledge, understanding and skills to the five learning outcomes
- develop transferable skills through their application within the context of achieving the learning outcomes

DRAFT

© WJEC CBAC Ltd 2027.

- develop literacy, numeracy and digital skills through their application within the context of achieving the learning outcomes
- develop knowledge and understanding of the key theories and principles which support effective practice in the subject, including:
  - data-informed and evidence-based practice, using accurate data, reliable sources and system information to support decisions, recommendations and improvements
  - computational thinking, applying logical sequencing, pattern recognition, abstraction and problem-solving when analysing data, programming and configuring systems
  - systems thinking, understanding how data, software, hardware and networks interact and how changes affect overall system performance
  - secure-by-design principles, protecting confidentiality, integrity and availability through appropriate access control, authentication and configuration
  - iterative development and testing, planning, testing, reviewing and refining solutions to improve accuracy, functionality and reliability
  - automated and AI-enabled systems to support interpretation, coding, configuration and research, while maintaining human oversight, validation and professional responsibility
  - responsible and ethical digital practice, handling data and security information appropriately, respecting privacy, verifying information and acknowledging sources
  - clear, audience-appropriate communication, presenting findings, risks and recommendations clearly using written, visual and digital formats
  - quality assurance and validation, checking accuracy, reviewing outputs (including AI-generated content), and ensuring solutions meet intended requirements
  - efficient and sustainable digital practice, using digital tools, systems and resources effectively and responsibly.

1.2. Prior learning and progression

There are no specific prior learning requirements for this qualification. It is designed primarily for learners aged 16 to 19 who wish to undertake study in a broad vocational area and prepare for progression to Level 3 study.

Learners may enter the qualification having previously achieved Level 1 or Level 2 qualifications, including GCSEs and other vocational or technical qualifications, or through relevant prior learning and experience.

The qualification is intended primarily to support progression to Level 3 study, including A Levels, V Levels, T Levels and other technical, vocational and academic qualifications, where appropriate. It provides a suitable foundation for further learning by enabling learners to develop and demonstrate knowledge, understanding and skills within a broad vocational area.

Achievement in the qualification can support progression decisions by schools, colleges and other education and training providers, helping learners make informed choices about their future educational pathways.

© WJEC CBAC Ltd 2027.

1.3. Guided Learning Hours (GLH) and Total Qualification Time (TQT)

Foundation Certificate in Digital Systems and Data has been designed to be delivered within 300 guided learning hours. The qualification has been designed as a 1-year programme for post-16 learners. Centres have flexibility in how they structure and deliver their courses within the total GLH for the qualification. The amount of content within each content area and its weighting within the qualification provides an indication of the anticipated percentage of GLH that may be required for each content area.

	Weighting	GLH
Content Area 1	40%	120
Content Area 2	24%	72
Content Area 3	36%	108
Totals	**100%**	**300 hours**

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:

- the number of hours which an awarding organisation has assigned to a qualification for Guided Learning
- 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.

The total qualification time for this qualification has been calculated as 400 hours. This includes:

- 300 hours of guided learning and supervised assessment
- 100 hours of non-supervised assessment related activities (for example independent research undertaken to support a supervised assessment task).

1.4. Use of language

As our understanding of diversity, equity, and inclusion evolves, so must our language. Terminology will be updated as needed to ensure it reflects individual identities and fosters respect and accuracy. Language used will be specific as possible. Staying informed and adaptable is crucial, as inclusive language promotes dignity and equity. Recognising that language will continue to evolve, we will remain open to further amendments to ensure it accurately represents and supports all individuals. We will inform centres of any amendments and the most up to date version of the specification will always be on the website.

© WJEC CBAC Ltd 2027.

1.5. Equality and fair access

This qualification is designed to be accessible to all learners, regardless of gender, ethnicity, religion, culture, or any other protected characteristic as defined by the Equality Act 2010. These characteristics include age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, and sexual orientation. Inclusive design principles have been applied throughout the qualification, including the use of varied assessment formats, clear and unbiased language, and diverse examples that reflect the breadth and diversity of the digital sector. Every effort has been made to avoid, where possible, features that could unjustifiably create barriers to access or achievement.

Access arrangements and reasonable adjustments are available for eligible learners to ensure they can participate fully in assessments and demonstrate their knowledge and skills. These adjustments do not alter the intended demand of the assessment but support fair access. Guidance on access arrangements and reasonable adjustments is provided in the Joint Council for Qualifications (JCQ) document *Access Arrangements, Reasonable Adjustments: General and Vocational Qualifications*, available at www.jcq.org.uk.

This qualification adheres to the principles outlined in the JCQ guidance. As a result of inclusive design and provision for reasonable adjustments, very few learners should encounter a complete barrier to any part of the assessment process.

DRAFT

© WJEC CBAC Ltd 2027.

2. Content areas

2.1. Content area format

GLH	Indicates the estimated number of hours a learner will spend under direct supervision or instruction. This includes classroom teaching, practical activities, supervised study and accompanying assessment.
Overview of content area	Provides a concise summary of the content's purpose, scope, and relevance. It outlines the key themes, skills, and knowledge areas covered.
Learning outcomes	Lists the learning outcomes that are covered by the content area.
Summary of assessment	Summarises the assessment methods for the content area.
Resources required for assessment	Details the materials, equipment, and facilities needed to carry out the assessment effectively. This ensures consistency and fairness in delivery across centres.
Amplification	Outlines the knowledge, understanding, and skills that learners need to be taught.

2.2. How to read the amplification

The amplification provided in the right-hand column uses the following two/three stems to indicate the expected depth of learning.

'Learners should know' is used when learners are expected to acquire and demonstrate knowledge through the recall, recognition or identification of facts, terms, features, processes or other subject content.

'Learners should understand' is used when learners are expected to demonstrate comprehension and understanding by explaining, interpreting, describing or discussing concepts, principles, theories, processes or information.

'Learners should know and understand' is used when learners are expected to acquire and demonstrate knowledge and understanding of concepts, principles, theories, processes or information. This includes being able to recall, describe, explain, interpret and discuss what they have learned.

2.3. Teaching content

Teaching content is provided for each topic, outlining the knowledge, understanding, and skills that learners need to be taught.

All content must be delivered unless otherwise indicated:

- the use of 'including' indicates that the specified content is mandatory and may be assessed. Centres may also choose to incorporate additional content or examples beyond those listed
- the use of 'for example' or 'such as' indicates that the specified content is provided for guidance only, and alternative examples may be used.

© WJEC CBAC Ltd 2027.

DRAFT

Content Area 1: Foundations of Digital Systems and Data

GLH	120
Overview of content area	This content area introduces learners to core knowledge about digital systems and data. It provides foundational of knowledge and understanding of data cleansing, analysis and presentation, configuration and security of digital systems, and the development, testing and deployment of a digital system. This content area is designed to prepare learners for the corresponding practical skills in Content Area 2 and Content Area 3. The purpose of this unit is to: • introduce fundamental data cleansing methods and tools to facilitate effective interpretation of raw data • develop the ability to communicate findings effectively to an audience • develop an understanding of standard configuration and security measures in digital systems • develop an understanding of systems development processes • introduce a range of testing strategies to effectively test a system prior to deployment • develop knowledge of key hardware components in a digital system and their interaction within a larger network. • develop understanding of communication and presentation methods appropriate to digital system deployment and management.
Learning outcomes	Learners to apply their knowledge and understanding of the following: • LO1 Clean, interpret and visualise a dataset in order to answer a question and communicate findings clearly • LO2 Configure and secure digital systems by applying access, authentication and configuration measures • LO3 Plan, develop and test a programming solution in order to meet a brief • LO4 Plan and configure hardware and software components in order to deliver a functional digital system • LO5 Select and apply reliable digital sources to produce evidence-based recommendations for an intended purpose
Summary of assessment	External assessment (paper based) Set and marked by WJEC
Resources required for assessment	There are no specific requirements for assessment.

© WJEC CBAC Ltd 2027.

Content

LO1 Clean, interpret and visualise a dataset in order to answer a question and communicate findings clearly

Learners will gain knowledge and understanding in the following areas:
KU1.1: Categorical, date or time, numerical, and text data types
KU1.2: Digital data sources comprising databases, online data repositories, spreadsheets, survey outputs and system-generated reports
KU1.3: The role of database structures and fields used to organise and retrieve structured data
KU1.4 The effect of duplicate records, inconsistent formatting, incorrect data types and missing values on accuracy and interpretation
KU1.5: The efficient use, storage and handling of data to support responsible and sustainable digital practices
KU1.6: The role of graphical and tabular formats, including their use within infographics, in supporting interpretation and communication of findings
KU1.7: The role of automated and AI-enabled features, data presentation tools and spreadsheets in supporting interpretation and presentation of data
KU1.8: The role of emerging digital technologies in shaping digital systems and services
KU1.9: The contribution of clear written and visual communication when presenting findings

Section	Amplification

KU1.1
Categorical, date or time, numerical, and text data types
	Learners should know:
	• the definitions of standard data types and formats:
	  • Boolean
	  • currency
	  • date and time
	  • integer
	  • float
	  • percentage
	  • text.
	• that data can be categorical, where data can be grouped into distinct categories, such as:
	  • nominal – data with no natural order or ranking
	  • ordinal – data with meaningful order or ranking.
	
	Learners should understand how these data types and categories are used and suggest appropriate data types for fields identified in examples of raw data.

DRAFT

© WJEC CBAC Ltd 2027.

KU1.2 Digital data sources comprising databases, online data repositories, spreadsheets, survey outputs and system-generated reports	Learners should know the advantages and disadvantages of the main types of digital data sources: • databases • online data repositories • reports automatically produced by a digital system • spreadsheets • survey outputs. Learners should understand the advantages and disadvantages of these digital data sources when formulating answers to questions, with relation to: • accuracy • completion rates • reliability.
KU1.3 The role of database structures and fields used to organise and retrieve structured data	Learners should know how to identify the fundamental characteristics of database structures, including: • fields • records • tables. Learners should understand the need for raw data to be organised and structured in order to: • enable efficient searching and sorting • facilitate effective analysis • improve consistency • reduce data duplication.

KU1.4
The effect of duplicate records, inconsistent formatting, incorrect data types and missing values on accuracy and interpretation
	Learners should know the effects of:
	• duplicate records:
	  • incorrect or misleading results from calculations, such as averages, totals and percentages
	  • slower processing
	  • wasted storage space
	• inconsistent formatting:
	  • data cannot be exported as effectively
	  • data is more difficult to interpret
	  • searching and filtering may be ineffective
	• incorrect data types:
	  • incorrect or misleading results from calculations or comparisons
	  • ineffective validation routines
	  • loss of data integrity
	  • sorts may not be applied consistently, leading to inaccurate analysis
	• missing values:
	  • incorrect or misleading results from calculations, such as averages, totals and percentages
	  • reduced accuracy of analysis due to an incomplete picture
	  • reduced data reliability and confidence in the analysis.
	
	Learners should understand how to prevent the following issues relating to raw data:
	• duplicate records:

© WJEC CBAC Ltd 2027.

	• identify unique records with a primary key • implement drop-down lists for data entry • inconsistent formatting • remove unnecessary duplicates • incorrect data types: • implement appropriate data types to fields • replace invalid entries manually or using automated or AI tools • missing values: • making important fields mandatory at point of entry • provide clear guidance on data collection forms.
KU1.5 The efficient use, storage and handling of data to support responsible and sustainable digital practices	Learners should know: • methods of efficient use, storage and handling of data, including: • avoiding collecting data unnecessarily • removal of duplicate entries • regularly updating outdated information • the use of searching, sorting and filtering tools to access data quickly • validating data at point of entry. • the advantages of efficient use, storage and handling, including: • faster data retrieval • improved compliance with data governance and retention requirements • improved quality and reliability of data • lower costs for data storage and management • reduced energy consumption associated with storing and processing data • reduced environmental impact through more sustainable digital practices • reduced storage requirements. • the potential disadvantages of not implementing efficient use, storage and handling, including: • comprehensive validation methods increase the time taken for data entry • genuine records can be removed if duplicate values are identified incorrectly • inaccurately applied search terms, filters or search criteria may hide important data • required data may not be available in the future if data collection is minimised • updating data is time and resource intensive.

DRAFT

© WJEC CBAC Ltd 2027.

KU1.6
The role of graphical and tabular formats, including their use within infographics, in supporting interpretation and communication of findings
	Learners should know the purpose of charts, graphs, infographics and tables to support interpretation and communication of findings including:
	• charts and graphs:
	  • accommodate categorical comparison (bar charts)
	  • allow trends to be visualised (line graphs)
	  • highlight outliers or anomalous results
	  • illustrate proportion (pie charts)
	  • improve understanding of large datasets
	• infographics:
	  • communicate findings quickly
	  • increase engagement by improving audience interest
	• tabular formats:
	  • allow precise comparison
	  • enable effective sorting and filtering
	  • organise data in a clear structure.
	
	Learners should understand the benefits of using these formats:
	• graphical:
	  • facilitates identification of patterns, trends and relationships
	  • improves accessibility of complex information
	  • supports rapid interpretation of findings
	• infographic:
	  • combines multiple forms of information in a single visual representation
	  • enhances communication with different audiences
	  • increases engagement and retention of key messages
	• tabular:
	  • enables accurate presentation of detailed data
	  • facilitates comparison between values and categories
	  • supports efficient sorting, analysis, filtering and sorting of data.

KU1.7
The role of automated and AI-enabled features, data presentation tools and spreadsheets in supporting interpretation and presentation of data
	Learners should understand the purpose of the following in supporting interpretation and presentation of data:
	• automated and AI-enabled features:
	  • identify patterns, trends and anomalies automatically
	  • generate visualisations and reports to communicate findings
	• data presentation tools:
	  • identify and summarise patterns, trends and relationships within data using data visualisation software
	  • when configured, communicate information clearly and effectively to the intended audience
	• spreadsheets:
	  • enable analysis, filtering and sorting
	  • organise data in a clear and structured format for easy interpretation.

© WJEC CBAC Ltd 2027.

KU1.8
The role of emerging digital technologies in shaping digital systems and services
	Learners should know the definitions and purpose of:
	• artificial Intelligence (AI):
	  • technology that enables computer systems to perform tasks that normally require human intelligence
	  • is used to analyse data, recognise patterns and support automated decision making
	• cloud computing:
	  • availability of computer resources, applications and data storage over the internet
	  • provides scalable access to services, data, processing and services across many locations and devices
	• the Internet of Things (IoT):
	  • a network of physical devices connected to the internet, collecting and sharing data
	  • enables monitoring, data collection and automation through connected devices and sensors.
	
	Learners should understand how emerging digital technologies shape digital systems and services:
	• artificial intelligence (AI):
	  • enables digital systems to make predictions, recognise patterns and support decision making
	  • improves digital services through automation and intelligent assistants
	  • reduces manual processes
	• cloud computing:
	  • storing and accessing data and software services over the internet
	  • supports scalable collaboration and data sharing between individuals and organisations
	• the Internet of Things (IOT):
	  • connects devices to collect and exchange data
	  • monitors and supports control of environments and systems in real time.

KU1.9
The contribution of clear written and visual communication when presenting findings
	Learners should know the contribution of clear visual and written communication when presenting findings, including clear:
	• visual communication:
	  • highlighting key anomalies, patterns and trends so findings can be understood quickly
	  • selecting appropriate charts, graphs and visualisations to present data effectively
	  • using colour, labels and titles consistently to aid interpretation
	• written communication:
	  • accurate spelling, grammar and punctuation to ensure meaning is clear
	  • structuring information using headings to improve readability and understanding
	  • using appropriate, clear and concise language to communicate findings to the intended audience.

DRAFT

© WJEC CBAC Ltd 2027.

Transferable skills

LO1	Analytical reasoning	Recording info	Clear communication	Numeracy	Digital capability
KU1.1	✓	✓		✓	
KU1.2	✓				
KU1.3	✓	✓	✓		
KU1.4	✓			✓	
KU1.5					✓
KU1.6	✓	✓	✓		
KU1.7	✓	✓	✓	✓	
KU1.8	✓				✓
KU1.9		✓	✓		

Work-related behaviours

LO1	**Attention to detail**	**Persistent**	**Reliable**
KU1.1	✓		
KU1.2			
KU1.3	✓		
KU1.4	✓		
KU1.5		✓	✓
KU1.6	✓		
KU1.7			✓
KU1.8	✓		
KU1.9	✓		

DRAFT

© WJEC CBAC Ltd 2027.

LO2 Configure and secure digital systems by applying access, authentication and configuration measures

Learners will gain knowledge and understanding in the following areas:

KU2.1: The operation of digital networks through connected devices, infrastructure components and software governed by communication protocols

KU2.2: Communication between devices and connected systems within digital networks

KU2.3: The meaning of confidentiality, integrity and availability in relation to protecting data, systems and services

KU2.4: The causes and indicators of security weaknesses and risks arising from insecure access, misconfigured system or network settings, unpatched software and weak authentication methods

KU2.5: Access permissions, authentication measures, configuration settings and protective controls in securing digital systems

KU2.6: The role of workplace policies and procedures in supporting secure system use and incident management: acceptable use policies, access control and authentication requirements, incident reporting and escalation procedures, data protection requirements, privacy and confidentiality requirements

KU2.7: Communication protocols, IP addressing conventions, secure configuration baselines and patch management practices in supporting secure and reliable digital systems

KU2.8: The use of automated security tools, dashboards, log files and monitoring information in identifying potential weaknesses and supporting system security

KU2.9: The role of digital tools, automated security scanning tools and AI-enabled systems in supporting secure configuration and identifying potential vulnerabilities, and the need to interpret, review and validate outputs before use

KU2.10: Health, safety and secure handling requirements when setting up, configuring or maintaining digital systems and equipment

Section	Amplification

KU2.1
The operation of digital networks through connected devices, infrastructure components and software governed by communication protocols
 	
KU2.2
Communication between devices and connected systems within digital networks
	Learners should know:
	• the purpose of digital networks in connecting devices and sharing data
	• the difference between local area networks (LANs) and wide area networks (WANs)
	• the role of key communications network infrastructure, including:
	  • routers
	  • switches
	  • wireless access points
	  • wired and wireless connections
	• communication protocols, including:
	  • HTTP/HTTPS
	  • MQTT
	  • TCP/IP.

KU2.3 The meaning of confidentiality, integrity and availability in relation to protecting data, systems and services	Learners should know the following principles of information security: • availability: ensuring that data, systems and services are accessible and operational when required by authorised users • confidentiality: ensuring that data is only accessible to authorised users, devices and systems • integrity: ensuring data remains accurate, complete and consistent, unless altered by authorised actions.

© WJEC CBAC Ltd 2027.

	Learners should understand how these principles contribute to protecting data, systems and services: • availability: helps to ensure continuity of service and access to information • confidentiality: helps to prevent unauthorised access, disclosure or misuse of information • integrity helps to maintain trust in the data by preventing accidental or deliberate modification.

KU2.4
The causes and indicators of security weaknesses and risks arising from insecure access, misconfigured system or network settings, unpatched software and weak authentication methods
	Learners should know the following security weaknesses:
	• insecure access:
	  • causes:
	  • incorrectly assigned user permissions
	  • misconfigured system or network settings
	  • unsecured ports
	  • indicators:
	  • users having access to data or systems beyond their intended access level
	  • unusual activity in systems or documents containing sensitive data
	  • risks:
	  • breaches of GDPR
	  • data loss, theft or misuse
	  • unauthorised access to systems and data
	• misconfigured systems or network settings:
	  • causes:
	  • human error when entering configuration values
	  • failure to follow installation/setup processes
	  • software updates or patches applied incorrectly
	  • indicators:
	  • slow network performance
	  • services or applications failing to start
	  • users unable to access files or network resources
	  • risks:
	  • data loss or corruption
	  • reduced system performance or reliability
	  • unauthorised access to files or network resources
	• unpatched software:
	  • causes:
	  • unpatched and out of date software versions
	  • using unsupported or outdated software
	  • indicators:
	  • increased security alerts
	  • missing security updates
	  • risks:
	  • incompatibility with security software
	  • malware installation
	  • unauthorised system access
	• weak authentication methods:
	  • causes:
	  • lack of multi-factor authentication
	  • lack of password complexity requirements
	  • indicators:
	  • use of simple or common passwords

© WJEC CBAC Ltd 2027.

DRAFT

	• repeated unsuccessful login attempts • unauthorised account activity • risks: • data loss, theft or misuse • identity theft or impersonation • unauthorised access to systems and data.
KU2.5 Access permissions, authentication measures, configuration settings and protective controls in securing digital systems	Learners should know the following security measures: • access permissions: • document permissions • read/write permissions • role-based access rights • user accounts and access levels • authentication measures: • biometric authentication • multi-factor authentication (MFA) • usernames and passwords • configuration settings: • prevent unauthorised actions that could compromise security • password policies • user device functionality restrictions • protective controls: • anti-malware software • backup procedures • firewalls • software updates. Learners should understand how these security measures can be used to secure a digital system.
KU2.6 The role of workplace policies and procedures in supporting secure system use and incident management: acceptable use policies, access control and authentication requirements, incident reporting and escalation procedures, data protection requirements, privacy and confidentiality requirements	Learners should know and understand the key workplace policies and procedures used to maintain secure system use and incident management: • access control and authentication requirements: • authentication requirements, including multi-factor authentication (MFA) • acceptable use policies: • user responsibilities when accessing organisational resources, such as: • keeping login credentials secure • logging out of shared devices • only accessing data appropriate to their role • incident reporting and escalation procedures through appropriate channels: • escalating incidents according to their severity • recording details of incidents • roles and responsibilities of staff during an incident • data protection, privacy and confidentiality requirements: • actions are in line with GDPR and The Data Protection Act 2018 • maintain confidentiality of information • protect personal, sensitive and organisational data from leaks.

© WJEC CBAC Ltd 2027.

	Learners should know the consequences of non-compliance with these key workplace policies and procedures, such as: • disciplinary action • legal action • loss of access rights • incident reporting protocols and escalation procedures. Learners should understand why these workplace policies and procedures are fundamental to operating digital systems in a secure, legal and sustainable manner.

KU2.7
Communication protocols, IP addressing conventions, secure configuration baselines and patch management practices in supporting secure and reliable digital systems
	Learners should understand how the following contribute to a secure and reliable digital system:
	• communication protocols:
	  • enable devices and services to exchange data reliably and consistently
	  • use secure protocols such as HTTPS to help protect data during transmission
	• IP addressing conventions:
	  • support accurate identification and communication between devices on a network
	  • help data reach the correct destination and supporting network management and troubleshooting
	• patch management practices:
	  • ensure software, operating systems and firmware are kept up to date
	  • reduces the risk of security vulnerabilities being exploited and improving system reliability and performance
	• secure configuration baselines:
	  • provide a standard set of secure system settings
	  • reduces vulnerabilities caused by misconfiguration and promoting consistent security across devices and services.

KU2.8
The use of automated security tools, dashboards, log files and monitoring information in identifying potential weaknesses and supporting system security
	Learners should know and understand the use of network management software and tools in identifying potential weaknesses and supporting system security:
	• automated security tools:
	  • continuously scan, monitor and analyse systems to detect vulnerabilities, suspicious or unusual activity and known threats
	  • allow faster identification and response to security risks.
	• dashboards:
	  • presents security and system information in a clear and accessible format
	  • enables administrators to monitor trends and user activity
	  • identifies risks and respond to potential issues effectively
	• log files:
	  • maintains a record of events and user actions
	  • supports the investigation of security incidents, the identification of vulnerabilities and the detection of unusual or unauthorised activity
	• monitoring information:

© WJEC CBAC Ltd 2027.

	• provides real-time and historical data about system performance, user activity and resource usage • helps to identify unusual behaviour, security incidents and potential system failures.
KU2.9 The role of digital tools, automated security scanning tools and AI-enabled systems in supporting secure configuration and identifying potential vulnerabilities, and the need to interpret, review and validate outputs before use	Learners should know the purpose of these different digital tools in supporting secure configuration through: • automatically checking systems against approved security baselines and identifying configuration weaknesses • detecting misconfigured devices, applications or services that may increase security risks • recommending or applying configuration changes to address vulnerabilities and improve compliance with security requirements. Learners should know how these different digital tools can be used to identify potential vulnerabilities: • continuously scanning systems, networks and applications to identify known vulnerabilities and security weaknesses • detecting unusual activity that may indicate misconfigurations, security weaknesses or emerging threats • analysing large volumes of security and system data more quickly than would be possible through manual reviews • enabling earlier detection of weaknesses, allowing organisations to reduce risk and respond more quickly to security issues. Learners should understand the need to interpret, review and validate outputs from these different digital tools.

KU2.10
Health, safety and secure handling requirements when setting up, configuring or maintaining digital systems and equipment
	Learners should know the key requirements when setting up, configuring or maintaining digital systems and equipment:
	• health and safety requirements:
	  • carrying out risk assessments before installing, moving or maintaining equipment
	• electrical safety:
	  • managing cables
	  • PAT testing of electrical devices
	  • ensuring equipment is switched off before maintenance where appropriate
	  • reporting damaged cables, plugs or devices
	  • using electrical equipment safely
	• protecting devices from damage, loss and theft through secure handling and physical methods.

DRAFT

© WJEC CBAC Ltd 2027.

Transferable skills

LO2	Problem solving	Recording technical information	Communication	Digital capability
KU2.1				✓
KU2.2				✓
KU2.3			✓	
KU2.4	✓			
KU2.5	✓			✓
KU2.6	✓	✓	✓	✓
KU2.7	✓			
KU2.8	✓	✓	✓	✓
KU2.9	✓	✓		✓
KU2.10		✓	✓	

Work-related behaviours

LO2	**Responsible**	**Perceptive**	**Attention to detail**
KU2.1			
KU2.2			
KU2.3	✓		
KU2.4	✓	✓	✓
KU2.5	✓	✓	
KU2.6	✓		
KU2.7			✓
KU2.8	✓	✓	
KU2.9	✓		✓
KU2.10	✓	✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

LO3 Plan, develop and test a programming solution in order to meet a brief	
Learners will gain knowledge and understanding in the following areas: KU3.1: The stages of programming solution development and their role in meeting an intended purpose KU3.2: The role of algorithms as ordered instructions that determine solution behaviour KU3.3: The relationship between algorithms, program code and solution outputs KU3.4: The role of structured logic and algorithms in the design of digital solutions KU3.5: The use of developer-written and externally sourced code within digital solutions and the need to comply with licensing requirements KU3.6: The effect of incorrect conditions, logic errors and syntax errors on program behaviour KU3.7: The role of automated and AI-enabled tools in generating code suggestions, and the need to review, test and understand these outputs before use KU3.8: The role of testing approaches in confirming that programming behaves as expected	
Section	**Amplification**

KU3.1
The stages of programming solution development and their role in meeting an intended purpose
	Learners should know the main stages of the system development lifecycle:
	• investigation and analysis:
	  • identifying the purpose of a system
	  • gathering and interpreting user requirements
	  • defining success criteria
	• design:
	  • creating user interface designs
	  • designing algorithms to meet user requirements using pseudocode and flowcharts
	  • planning inputs, processes and outputs
	• implementation:
	  • creating programmed solutions utilising iterative user feedback
	• testing:
	  • testing a solution using suitable test data
	  • identifying and correcting errors
	  • testing against user requirements
	• refinement:
	  • correcting and improving a system after implementation
	  • adapting the system to changing user requirements.

KU3.2
The role of algorithms as ordered instructions that determine solution behaviour
 	
KU3.3
The relationship between algorithms, program code and solution outputs
	Learners should know:
	• that an algorithm is a set of logical steps to solve a problem using:
	  • the order of instructions to determine how a solution operates and the results it produces
	  • constructs such as sequence, selection and iteration.
	• the relationship between algorithms, program code and solution outputs:
	  • algorithms – define the steps needed to solve a problem
	  • program code – implements an algorithm
	  • solution outputs – are produced when code is executed.

© WJEC CBAC Ltd 2027.

	Learners should understand how well-designed algorithms lead to more effective program code and produce appropriate system outputs in any given scenario.
KU3.4 The role of structured logic and algorithms in the design of digital solutions	Learners should know the purpose of structured logic and algorithms in the design of digital solutions, including: • structured logic determines how decisions and actions are carried out based on inputs and conditions • algorithms provide the logical order of instructions needed to process data and solve problems efficiently.

KU3.5
The use of developer-written and externally sourced code within digital solutions and the need to comply with licensing requirements
	Learners should know:
	• the main uses of code from different sources within digital solutions including:
	  • developer-written code:
	  • created specifically to meet the requirements of a particular solution or user need
	  • developed and maintained by the programmer or development team responsible for the solution
	  • provides greater control over functionality, performance and security
	  • externally sourced code:
	  • code, libraries or templates obtained from third parties
	  • incorporates pre-written and tested functionality
	  • may provide specialised features or capabilities that would be complex to develop from scratch
	• the advantages of reusing existing code or utilising externally sourced code including:
	  • reducing development time by using pre-existing, tested components rather than creating all code from scratch
	  • reducing development costs and effort by avoiding duplication of work
	  • enabling developers to make use of specialist functionality without needing to develop complex features themselves
	• the disadvantages of reusing existing code or utilising externally sourced code including:
	  • externally sourced code may contain vulnerabilities or malicious code that are not immediately apparent
	  • the quality, reliability and accuracy of third-party code cannot always be guaranteed
	  • reused code may contain unnecessary features, increasing system complexity and maintenance requirements
	• the main licensing implications of using code including:
	  • ensuring code use is in line with licensing or acceptable use policies from the original developer
	  • recognition of intellectual property where required
	  • the legal, professional and reputational consequences of using code without permission.

DRAFT

© WJEC CBAC Ltd 2027.

KU3.6
The effect of incorrect conditions, logic errors and syntax errors on program behaviour
	Learners should know that coding errors can produce incorrect or unexpected system outputs and syntax errors should stop the program from running.
	
	Learners should understand the causes of:
	• logic errors:
	  • incorrect selection conditions
	  • incorrect operators used in calculations
	  • missing or incorrect loop stop conditions
	• syntax errors:
	  • incorrect use of language-specific commands
	  • invalid variable names
	  • missing operators
	  • spelling mistakes in source code.

KU3.7
The role of automated and AI-enabled tools in generating code suggestions, and the need to review, test and understand these outputs before use
	Learners should know:
	• that an Integrated Development Environment (IDE) may provide the programmer with automatically generated, or AI-generated code suggestions and live debugging of code
	• the advantages of using automated or AI-enabled tools for generating code suggestions, such as:
	  • assisting developers by suggesting appropriate code or functions
	  • reducing development time by generating/auto-completing routine or repetitive sections of code
	  • the disadvantages of using automated or AI-enabled tools for generating code suggestions, such as:
	  • generated code may contain errors, inefficiencies or vulnerabilities that are not immediately obvious
	  • suggestions may not fully meet the requirements of the intended solution or user needs
	  • overreliance on automated tools may reduce a developer's understanding of programming concepts and problem-solving skills
	  • generated code can be difficult to understand, modify or maintain.
	
	Learners should understand that AI or automatically generated code may not be fit for purpose and therefore there is a need to review, test and understand these outputs before use.

DRAFT

© WJEC CBAC Ltd 2027.

KU3.8
The role of testing approaches in confirming that programming behaves as expected
	Learners should know:
	• the purpose of white box testing and black box testing
	• the importance of black box testing, to establish whether:
	  • all functions and features operate as intended from an end-user perspective
	  • the solution behaves consistently under different usage scenarios
	  • the solution is suitable for acceptance by users and ready for deployment
	  • user and system requirements have been met.
	
	Learners should understand how test data is used in white box testing to check a system works as intended, including:
	• typical
	• extreme
	• erroneous.

Transferable skills

LO3	Problem solving	Planning and organisation	Communication	Digital capability
KU3.1		✓		
KU3.2	✓	✓		✓
KU3.3	✓		✓	✓
KU3.4	✓	✓	✓	✓
KU3.5		✓		✓
KU3.6	✓		✓	✓
KU3.7	✓			✓
KU3.8	✓	✓	✓	✓

Work-related behaviours

LO3	**Persistent**	**Focused**	**Adaptable**
KU3.1	✓		✓
KU3.2			
KU3.3	✓	✓	
KU3.4		✓	✓
KU3.5	✓	✓	✓
KU3.6	✓		
KU3.7			✓
KU3.8	✓	✓	✓

© WJEC CBAC Ltd 2027.

LO4 Plan and configure hardware and software components in order to deliver a functional digital system

Learners will gain knowledge and understanding in the following areas:

KU4.1: The role of planning tasks, sequencing activities and allocating resources when delivering a digital system

KU4.2: The interaction between hardware and software components in enabling system functionality

KU4.3: The role of user interface elements, accessibility and digital content in supporting the usability of a digital system

KU4.4: The role of component compatibility and system requirements in configuring a functional digital system

KU4.5: The influence of dependencies between components on overall system operation

KU4.6: The occurrence of faults during configuration and operation and the need for checking, diagnosis and corrective action

KU4.7: The contribution of maintenance activities comprising updates, checks and troubleshooting to continued system performance and reliability

KU4.8: Factors that affect the energy use, resource efficiency and sustainability of digital systems and devices

KU4.9: The role of digital tools, automation features and automated AI-enabled systems in generating configuration and supporting system setup, and the need to check such outputs for suitability for the intended system

Section	Amplification
KU4.1 The role of planning tasks, sequencing activities and allocating resources when delivering a digital system	Learners should know the purpose of planning tasks to: • ensure requirements are met • identify timescales and milestones • monitor progress throughout development. Learners should know the purpose of sequencing activities to: • identify the order in which tasks need to be completed to achieve the desired outcome • recognise dependencies between activities, where one task must be completed before another can begin • schedule activities to ensure key milestones and deadlines can be met. Learners should know the categories of resources when developing digital systems: • budget • hardware • human resources • software • time. Learners should know the purpose of effective resource allocation to: • ensure the people, budget, equipment, people and software required for a task are available when needed • make efficient use of available resources to avoid delays • minimise wasted time, effort and expenditure through effective planning and coordination of resources.

© WJEC CBAC Ltd 2027.

	Learners should understand the consequences of insufficient planning and sequencing of development activities: • difficulties coordinating team members and allocating responsibilities effectively • increased risk of delays, missed deadlines and failure to meet project milestones • inefficient use of resources, resulting in duplicated effort and reduced productivity • reduced confidence in the quality, reliability and maintainability of the completed digital system.
KU4.2 The interaction between hardware and software components in enabling system functionality	Learners should know that hardware components are the physical parts of a digital system that facilitate system functionality through: • automatically inputted data from sensors • manually inputted data • processing of data • short and long-term storage of data • the display of system outputs. Learners should know that software provides instructions to hardware components. Learners should understand that: • hardware and software must be compatible to enable a digital system to operate correctly • software designed for one operating system, device type or hardware specification may not function correctly on another • hardware upgrades may require compatible drivers, operating systems or software updates to ensure continued operation.

KU4.3
The role of user interface elements, accessibility and digital content in supporting the usability of a digital system
	Learners should know the function of common:
	• user interface elements including:
	  • buttons
	  • check boxes
	  • drop down boxes
	  • icons
	  • menus
	  • pointers
	  • text fields
	  • windows
	• accessibility features including:
	  • adjustable font sizes
	  • colour filters
	  • customisable display settings
	  • screen reader compatibility
	  • text to speech
	  • transcripts
	  • visual notification alerts
	  • voice control

DRAFT

© WJEC CBAC Ltd 2027.

	Learners should know how digital content can support useability through: • making information easy to understand • supporting clear and consistent navigation • supporting different users • supporting users to complete tasks. Learners should understand how interface elements, accessibility features and digital content can support usability of a digital system.

KU4.4
The role of component compatibility and system requirements in configuring a functional digital system
	Learners should know the purpose of compatibility in a digital system in terms of compatibility between hardware and software components to ensure reliable operation and reduce the likelihood of faults occurring – this includes:
	• hardware with software requirements:
	  • software choice may be informed by hardware specifications in terms of:
	  • processor speed
	  • memory
	  • storage capacity
	• interconnected devices must be able to communicate effectively using compatible standards, such as:
	  • Bluetooth
	  • ethernet
	  • USB
	  • Wi-Fi
	• appropriate drivers may be required to operate non-standard peripheral devices.
	
	Learners should understand the consequences of not choosing compatible hardware or software on a digital system:
	• incompatible components may prevent a system from operating correctly or fulfilling its intended purpose
	• incompatible peripherals may create unnecessary configuration changes
	• software may not install or run correctly if hardware requirements are not met.

KU4.5
The influence of dependencies between components on overall system operation
	Learners should understand how dependencies affect system operation including:
	• a component requires data from another component, such as:
	  • a CPU depends on RAM to provide instructions and data currently being processed
	  • a display requiring processed data from the CPU before information can be shown
	  • an operating system depends on storage devices to access system files
	• components work together to produce system outputs or functions, such as:
	  • a keyboard, CPU and monitor work together to allow a user to enter and view data
	  • actuators, sensors and software working together to control a smart heating system

© WJEC CBAC Ltd 2027.

	• the operation of one component impacts the performance of another, such as:
	  • insufficient RAM may cause applications and the CPU to operate slowly
	  • limited storage capacity may reduce the ability to save files or install updates.
	
	Learners should know that component failure should result in reduced operation of the overall system and the system not meeting its intended purpose.

KU4.6
The occurrence of faults during configuration and operation and the need for checking, diagnosis and corrective action
	Learners should know:
	• the main types of faults that can occur during system configuration and operation:
	  • configuration errors
	  • hardware faults
	  • network faults
	  • software faults
	• why faults need to be checked to:
	  • facilitate diagnosis of system faults to inform corrective action
	  • identify unexpected behaviour
	  • verify operation in line with requirements
	• that fault diagnosis is required to understand the cause of faults and facilitate effective corrective action
	• the standard procedures for correcting faults:
	  • correcting configuration errors
	  • replacing faulty hardware or components
	  • updating or reinstalling software.

KU4.7 The contribution of maintenance activities comprising updates, checks and troubleshooting to continued system performance and reliability	Learners should know the contribution of these activities in relation to continued systems performance and reliability: • consistent checks to digital systems identify potential issues before they have a significant effect on system performance • troubleshooting in a digital system addresses problems as they occur, identifying the root cause and limiting future performance issues • updating system software and hardware contributes to a more secure digital system, less likely to be compromised by malicious software. Learners should understand the impacts of poorly maintained digital systems, such as: • greater risk of malware infections, unauthorised access and data breaches • increased likelihood of hardware failures due to wear, damage or inadequate maintenance • reduced system performance, including slower response times, longer loading times and reduced productivity.

© WJEC CBAC Ltd 2027.

KU4.8
Factors that affect the energy use, resource efficiency and sustainability of digital systems and devices
	Learners should know:
	• the main factors affecting energy use and efficiency of digital systems and devices, including:
	  • component and hardware efficiency ratings
	  • power management settings
	  • network usage
	• the main factors affecting the sustainability of digital systems and devices, such as:
	  • device lifespan
	  • maintenance and upgradeability
	  • methods of disposal and recycling.

KU4.9
The role of digital tools, automation features and automated AI-enabled systems in generating configuration and supporting system setup, and the need to check such outputs for suitability for the intended system
	Learners should know:
	• the purpose of using digital tools, automation and AI to:
	  • improve consistency of system performance
	  • reduce the risk of human error in applying configuration settings
	  • reduce workload on systems management staff
	• how digital tools, automation and AI can be used to aid set up and configuration of a digital system such as:
	  • applying access controls, firewalls rules and security baselines during system setup
	  • automatically detecting and configuring connected devices such as printers, storage devices and network hardware
	  • deploying standardised system configurations from predefined templates or configuration profiles
	  • using AI-powered assistants to recommend configuration settings based on organisational requirements or previous deployments.
	
	Learners should understand the need for human checks of automated or AI generated system settings and configurations to:
	• ensure that the system fulfils its intended purpose
	• maintain accountability and integrity
	• understand how the system functions to facilitate future maintenance.

DRAFT

© WJEC CBAC Ltd 2027.

Transferable skills

LO4	**Planning and organisation**	**Problem solving**	**Recording info**	**Digital capability**
KU4.1	✓	✓		
KU4.2		✓		
KU4.3			✓	✓
KU4.4	✓	✓	✓	✓
KU4.5	✓	✓	✓	✓
KU4.6		✓	✓	
KU4.7	✓	✓	✓	
KU4.8	✓		✓	
KU4.9	✓		✓	✓

Work-related behaviours

LO4	Organised	Flexible	Committed
KU4.1	✓		✓
KU4.2		✓	
KU4.3			
KU4.4	✓		
KU4.5	✓	✓	
KU4.6		✓	✓
KU4.7	✓	✓	✓
KU4.8	✓	✓	
KU4.9	✓		✓

DRAFT

© WJEC CBAC Ltd 2027.

LO5 Select and apply reliable digital sources to produce evidence-based recommendations for an intended purpose

Learners will gain knowledge and understanding in the following areas:
KU5.1: Variation in the accuracy, authority, purpose and reliability of digital information
KU5.2: The role of comparing information across multiple sources in supporting accurate conclusions
KU5.3: The influence of bias within digital information on interpretation and recommendations
KU5.4: The potential for automated and AI-enabled content generation systems to produce inaccurate, misleading or fabricated information (sometimes referred to as hallucinated outputs), and the need to verify such information against reliable sources
KU5.5: The importance of intellectual property rights, ownership, attribution and appropriate use of digital and AI-generated content
KU5.6: The role of referencing practices in ensuring transparency and traceability of sources
KU5.7: The role of workplace procedures governing acknowledgement and recording of information sources

Section	Amplification

KU5.1
Variation in the accuracy, authority, purpose and reliability of digital information
	Learners should know the factors that affect, accuracy, authority, purpose and reliability of digital information:
	• accuracy:
	  • completeness
	  • errors
	  • factual correctness
	• authority:
	  • published author/organisational credentials:
	  • recognised authors
	  • reputable sources
	• purpose:
	  • different audiences
	  • different contexts
	• reliability:
	  • differing information/source trustworthiness
	  • inconsistency of information
	  • information may not be up to date
	  • unverified sources.
	
	Learners should understand how these factors influence the suitability of digital information for organisational use.

KU5.2 The role of comparing information across multiple sources in supporting accurate conclusions	Learners should know the purpose of assessing the credibility and reliability of information sources, such as: • checking that information is supported by evidence, references or verifiable data • determining whether information comes from a trustworthy and authoritative source • identifying information that may be inaccurate, misleading or deliberately false. Learners should understand: • the need to compare source information by: • assessing credibility and reliability of different sources

© WJEC CBAC Ltd 2027.

	• assessing conflicting information from different sources • comparing evidence from different sources • these actions can improve confidence in conclusions, decisions and recommendations.
KU5.3 The influence of bias within digital information on interpretation and recommendations	Learners should know how bias in digital information can influence interpretation and recommendations, including: • presenting a limited or unbalanced view of a topic • reducing objectivity in decision making • leading to inaccurate or unsupported conclusions • influencing recommendations towards particular products, services or viewpoints. Learners should understand how bias can exist in digital information sources through: • financial incentive • organisational interests • personal opinion • political perspectives.

KU5.4
The potential for automated and AI-enabled content generation systems to produce inaccurate, misleading or fabricated information (sometimes referred to as hallucinated outputs), and the need to verify such information against reliable sources
	Learners should know that automated and AI-enabled content may be inaccurate or misleading due to:
	• fictitious sources
	• hallucinated outputs
	• incorrectly drawn conclusions
	• lack of reliable sources as a basis for generation
	• plausible but false information.
	
	Learners should understand:
	• the impact of relying solely on AI-enabled content including:
	  • inaccurate information may lead to poor decisions, incorrect conclusions
	  • important context, exceptions or alternative viewpoints may be overlooked
	  • users may become over-reliant on automated tools and apply less critical judgement.
	• the need to verify AI-generated information by:
	  • checking facts against reliable sources
	  • comparing conclusions or information across multiple sources
	  • validating the sources or references used in the generation of AI content.

DRAFT

© WJEC CBAC Ltd 2027.

KU5.5
The importance of intellectual property rights, ownership, attribution and appropriate use of digital and AI-generated content
	Learners should know:
	• the fundamentals of intellectual property rights and how they are applied to digital and AI-generated content:
	  • copyright:
	  • gives the creator legal rights over how their work is copied, distributed, modified or shared
	  • protects original creative works such as digital media, images, music, software, videos and written content
	  • licensing agreements:
	  • may restrict commercial use, redistribution, modification or the number of permitted users
	  • specify how software, digital resources, datasets and media can be used, shared or modified
	  • patents:
	  • protect new inventions, processes or technical solutions for a specified period
	  • prevent others from making, using or selling a patented invention without permission
	  • trademarks:
	  • help users identify genuine products, services and software from a particular organisation
	  • protect names, logos, symbols, slogans and brand identities that distinguish products or services
	• the concept of ownership in digital content in terms of:
	  • creator ownership – when the individual who creates digital content, software or other assets retains the legal rights and control over how that work is used, shared or modified
	  • organisational ownership – the organisation employing or commissioning the creator holds the rights to digital content, allowing it to control, distribute and manage their use
	• the purpose of attribution is to:
	  • acknowledge creators
	  • maintain professional integrity
	  • recognise contributors
	  • reference sources
	  • support transparency.
	
	Learners should understand the importance of appropriate use of digital and AI-generated content in terms of:
	• maintaining integrity and credibility
	• potential legal consequences
	• promoting ethical practice
	• respecting the work of others
	• supporting positive use of AI tools in digital industries.

DRAFT

© WJEC CBAC Ltd 2027.

KU5.6 The role of referencing practices in ensuring transparency and traceability of sources	Learners should know the purpose of referencing when creating and developing digital systems to: • maintain transparency • remain in line with legislation • support ethical practice • recognise digital creators appropriately • facilitate evaluation and review of a digital resource or system later.

KU5.7
The role of workplace procedures governing acknowledgement and recording of information sources
	Learners should know:
	• the purpose of workplace procedures in governing acknowledgement and recording of information sources to:
	  • demonstrate that information or data has been obtained from legitimate sources
	  • ensure information can be traced back to its original source
	  • give appropriate credit to the original creators, authors or organisations
	  • support compliance with copyright, licensing agreements and intellectual property rights
	• how workplace procedures help ensure information is used responsibly and appropriately through:
	  • acknowledging the use of AI content
	  • citing authors, organisations and publication dates
	  • producing reference lists
	  • referencing sources in reports and information materials.
	
	Learners should understand the consequences of not following these workplace procedures, including:
	• copyright, licensing or intellectual property rights may be breached, leading to legal or financial consequences
	• failure to acknowledge sources may result in plagiarism or the misrepresentation of work as original
	• the accuracy and credibility of findings, reports or recommendations may be questioned.

DRAFT

© WJEC CBAC Ltd 2027.

Transferable skills

LO5	Research skills	Analytical reasoning	Communication	Digital capability
KU5.1	✓	✓		✓
KU5.2	✓	✓		
KU5.3	✓	✓	✓	✓
KU5.4	✓	✓	✓	✓
KU5.5	✓	✓		
KU5.6	✓		✓	✓
KU5.7	✓			✓

Work-related behaviours

LO5	Perceptive	Reflective
KU5.1	✓	✓
KU5.2	✓	✓
KU5.3	✓	✓
KU5.4	✓	✓
KU5.5	✓	
KU5.6	✓	✓
KU5.7	✓	

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 2: Digital Data and Sources in Practice

GLH	72
Overview of content area	This content area is about learners using digital data and digital sources and they will be applying the LO1 and LO5 knowledge and understanding gained from Content Area 1 – develop an understanding of how components interact to meet defined purposes. Learners will: • work with structured datasets and clean, interpret and visualise data to answer defined questions • develop an understanding of how data is used to inform decisions within digital contexts • identify and assess the reliability of digital sources • develop the foundational skills needed to make evidence-based recommendations. The purpose of this unit is to: • develop the practical skills needed to prepare, interpret and visualise structured data to support informed decisions • develop the ability to identify patterns, draw conclusions and communicate findings clearly for different purposes and audiences • develop research skills to identify, compare and evaluate digital sources and select reliable evidence • develop the ability to use data and reliable digital information to make evidence-based recommendations in real-world digital contexts.
Learning outcomes	**LO1:** Clean, interpret and visualise a dataset in order to answer a question and communicate findings clearly **LO5:** Select and apply reliable digital sources to produce evidence-based recommendations for an intended purpose
Summary of assessment	Non-exam assessment. Externally set, internally marked, externally moderated
Resources required for assessment	• Suitable digital device with spreadsheet and data presentation tools • Appropriate digital storage for assessment evidence • Access to reliable internet and digital information sources

© WJEC CBAC Ltd 2027.

Content

LO1 Clean, interpret and visualise a dataset in order to answer a question and communicate findings clearly	
Learners will gain skills in the following areas: SK1.1: Format, clean and prepare digital datasets using spreadsheet and data presentation tools SK1.2: Review datasets for accuracy and resolve missing values, duplicate records, inconsistent formatting and incorrect data types SK1.3: Create charts and tables to represent data SK1.4: Identify patterns and draw conclusions SK1.5: Communicate findings clearly for an intended purpose Please note that the use of datasets relates to data contained in csv files.	
Section	**Amplification**

SK1.1
Format, clean and prepare digital datasets using spreadsheet and data presentation tools
	Learners should be able to use spreadsheet and data presentation tools to:
	• format digital datasets including:
	  • applying appropriate and consistent formats to, categorical, date or time numerical and text data types
	  • formatting data fields and tables consistently so that information is clearly presented and easily interpreted
	  • applying suitable styling and layout techniques
	• clean digital datasets including:
	  • identifying and correcting data entry errors
	  • correcting inconsistent representations of data values and formats
	  • applying consistent formats to data within fields and records
	• prepare digital datasets for quality assurance including:
	  • arranging data in a consistent and appropriate structure for analysis
	  • using sorting and filtering functions to organise data for a defined purpose
	• using search functions to locate and review relevant data.

SK1.2
Review datasets for accuracy and resolve missing values, duplicate records, inconsistent formatting and incorrect data types
	Learners should be able to review datasets and resolve data quality issues to ensure they can be interpreted and used appropriately for analysis.
	
	This should involve:
	• accuracy reviews:
	  • checking data values for errors, inconsistencies and unexpected entries
	  • comparing data against known standards, rules or available reference information where appropriate
	• resolving missing values:
	  • missing completely at random (MCAR)
	  • missing at random (MAR)
	  • missing not at random (MNAR)
	• resolving duplicate records by:
	  • identifying records containing the same information
	  • checking whether matching records represent duplicate entries or separate records

© WJEC CBAC Ltd 2027.

	• removing or correcting duplicate records where appropriate • resolving inconsistent formatting by: • identifying differences in the way equivalent data is represented within a dataset • standardising data formats so that equivalent values are represented consistently • checking that standardised values remain accurate and suitable for analysis • resolving incorrect data types by: • identifying values that do not match the intended data type for a field • changing values to the appropriate data type • correcting identified errors using verified information by: • entering missing values where the correct information can be established • identifying fields or records where expected data is absent • applying a consistent approach to values that cannot be established.
Preparation of data for interpretation and analysis SK1.3 Create charts and tables to represent data	Learners should be able to: • represent data: • in preparation for interpretation and analysis to answer a set question and for a specified audience • that is clear and appropriate for the intended purpose and audience • select the most appropriate format (chart or table) to represent the data most effectively • select data that is relevant to the purpose of the chosen format • ensure the selected format accurately represents the underlying data • create charts: • to represent comparisons, patterns or relationships • using suitable headings, labels, scales or titles where appropriate • create tables: • arranging data logically using appropriate columns, headings and rows • applying consistent formatting to make categories, labels and values clear • including appropriate summaries such as totals, averages, counts or percentages, or other calculated values where relevant.

DRAFT

© WJEC CBAC Ltd 2027.

Interpretation and analysis of data
 	
SK1.4
Identify patterns and draw conclusions
 	
SK1.5
Communicate findings clearly for an intended purpose
	Learners should be able to, in response to a set question and for a specified audience:
	• interpret data by identifying patterns
	• analyse data by drawing conclusions
	• communicate their findings clearly.
	
	They should be able to:
	• use datasets, charts, tables and any other relevant prepared data representations to support interpretation and analysis
	• select data for interpretation and analysis that is relevant to the question set
	• use numerical measures to support interpretation and analysis such as calculating and interpreting averages, proportions, totals where appropriate
	• identify patterns by:
	  • noting any appropriate trends or relationships
	  • comparing categories, groups or values to identify similarities and differences where appropriate
	  • noting any significant changes, repeats or values that may require further investigation
	• draw clear conclusions that are supported by the available data to distinguish between supported conclusions and those that cannot be supported by the available evidence
	• present findings:
	  • in a format appropriate to the intended purpose and audience for example, use suitable layout and language
	  • that use clear, consistent and appropriate communication skills.
	
	Learners should be able to communicate clearly through:
	• adaptation for the intended purpose and audience such as:
	  • identifying the information most relevant
	  • adapting language, layout, presentation and/or terminology as appropriate
	  • selecting the most appropriate format for communicating the findings
	• use of effective written communication:
	  • using clear, consistent and appropriate language
	  • organising information clearly using headings, sub-headings and labels
	  • summarising key findings and conclusions accurately and concisely
	  • selecting an appropriate level of detail and suitable terminology
	• use of effective visual communication:
	  • selecting appropriate tables, charts or other suitable visual formats to communicate relevant findings
	  • using visual presentation to highlight important information and support understanding
	  • combining written, tabular and graphical information where this supports understanding.

© WJEC CBAC Ltd 2027.

Transferable skills

LO1	Analytical reasoning	Recording information	Clear communication	Numeracy	Digital capability
SK1.1		✓			✓
SK1.2	✓	✓			✓
SK1.3		✓	✓	✓	✓
SK1.4	✓		✓	✓	
SK1.5		✓	✓		✓

Work-related behaviours

LO1	Attention to detail	Persistent	Reliable
SK1.1	✓		✓
SK1.2	✓	✓	✓
SK1.3	✓		✓
SK1.4		✓	✓
SK1.5	✓		✓

DRAFT

© WJEC CBAC Ltd 2027.

LO5 Select and apply reliable digital sources to produce evidence-based recommendations for an intended purpose

Learners will gain skills in the following areas:
SK5.1: Identify digital sources that are relevant to a defined purpose
SK5.2: Check information across sources to confirm key points
SK5.3: Select information that directly supports an evidence-based recommendation
SK5.4: Acknowledge and reference sources used
SK5.5: Communicate recommendations clearly, showing how evidence supports conclusions
SK5.6: Use checking, formatting and search functions within digital applications to support drafting, reviewing and organising information

Reference to 'information' means any data or background knowledge potentially relevant to the defined purpose.

Section	Amplification

SK5.1
Identify digital sources that are relevant to a defined purpose
	Learners should be able to identify information relevant to the defined purpose and assess digital sources by:
	• reviewing digital sources to identify information relevant to the defined purpose
	• assessing the currency, relevance, authority, accuracy and purpose of those sources such as:
	  • considering who produced the information and their expertise or authority
	  • checking whether information is supported by evidence or references
	  • checking important claims against other provided sources
	  • considering the purpose and possible bias of the information
	  • considering whether the information is current.

SK5.2 Check information across sources to confirm key points	Learners should be able to check information across sources, including: • identifying the key points that require confirmation • deciding whether key points are confirmed, contradicted or remain unresolved • locating corresponding information in another source • comparing information across sources to identify consistency, similarities and differences, omissions or contradictions • investigating any significant discrepancies by considering the available evidence • recording the outcome of checks clearly.

SK5.3
Select information that directly supports an evidence-based recommendation
	Learners should be able to:
	• select information from checked sources to support an evidence-based recommendation by:
	  • identifying information that directly addresses the defined purpose
	  • extracting relevant claims, data or evidence from the checked sources
	  • distinguishing between opinion and/or unsupported evidence and facts/supported evidence.

© WJEC CBAC Ltd 2027.

SK5.4
Acknowledge and reference sources used
	• acknowledge and reference sources used by:
	  • identifying the sources used in their work
	  • acknowledging any data, ideas, information obtained from sources
	  • providing sufficient information to allow sources to be identified
	  • using an appropriate and consistent referencing format, such as in-text citations, footnotes or a reference list.

SK5.5
Communicate recommendations clearly, showing how evidence supports conclusions
	Learners should be able to:
	• communicate recommendations clearly by:
	  • stating the recommendation in relation to the defined purpose
	  • using concise, accessible language and appropriate terminology for the intended audience
	• show how evidence supports conclusions by:
	  • identifying the relevant evidence
	  • explaining how the evidence supports the recommendation
	• present recommendations appropriately by:
	  • selecting an appropriate format
	  • organising the recommendation and supporting evidence so that the conclusion can be clearly understood.

SK5.6
Use checking, formatting and search functions within digital applications to support drafting, reviewing and organising information
	Learners should be able to use digital application functions to support drafting, reviewing and organising information by:
	• drafting and reviewing information:
	  • creating and refining a draft before it is finalised
	  • reviewing information for accuracy, relevance and completeness
	• using checking functions to:
	  • identify and correct errors such as spelling and grammar errors
	  • check consistency and completeness before information is finalised
	• using formatting functions to:
	  • organise information using headings, lists, tables and other appropriate formatting features
	  • apply consistent formatting to improve clarity and readability
	• using search functions to:
	  • locate relevant information within provided sources or their own work.

DRAFT

© WJEC CBAC Ltd 2027.

Transferable skills

LO5	Research skills	Analytical reasoning	Communication	Digital capability
SK5.1	✓			✓
SK5.2	✓	✓		✓
SK5.3	✓	✓		
SK5.4				✓
SK5.5			✓	✓
SK5.6		✓		✓

Work-related behaviours

LO5	Perceptive	Reflective
SK5.1	✓	
SK5.2	✓	✓
SK5.3	✓	✓
SK5.4		✓
SK5.5	✓	✓
SK5.6		✓

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 3: Digital Systems in Practice

GLH	108
Overview of content area	This content area develops learners' practical skills working with digital systems and they should be applying the LO2, LO3 and LO4 knowledge and understanding gained from Content Area 1 – making this synoptic in its approach. Learners should learn to: • configure systems, apply security measures, monitor system information, identify security weaknesses and respond appropriately to support the confidentiality, integrity and availability of data and services • work with defined problems and briefs to plan, develop and test coded solutions • build an understanding of how structured logic and algorithms are used to produce digital outcomes • work with hardware and software components to plan tasks and configure systems to produce a functional digital system. The purpose of this unit is to: • develop the practical skills needed to configure and secure digital systems by applying access, authentication and configuration measures • develop programming skills to plan, develop, test and refine solutions to meet a defined purpose • develop the ability to plan, configure and maintain hardware and software components to deliver functional digital systems • develop the ability to bring together programming, system configuration, testing and security skills to produce and communicate functional digital solutions in real-world digital contexts.
Learning outcomes	**LO2** Configure and secure digital systems by applying access, authentication and configuration measures **LO3** Plan, develop and test a programming solution in order to meet a brief **LO4** Plan and configure hardware and software components in order to deliver a functional digital system
Summary of assessment	Non-exam assessment, synoptic. Externally set, internally marked, externally moderated.
Resources required for assessment	• Access to suitable digital devices, software development tools, digital system configuration tools and a defined digital system or suitable simulated environment. • Learners should also require access to digital tools for recording, organising and communicating configuration, security, programming and maintenance information. • A consistent system or simulation in which learners can configure and check security settings, review logs, record findings and escalate a concern (see Appendix B for more detail).

© WJEC CBAC Ltd 2027.

Content

LO2 Configure and secure digital systems by applying access, authentication and configuration measures	
Learners will gain skills in the following areas: SK2.1: Configure digital systems by applying access controls, authentication requirements, permissions, security settings, secure configuration and update procedures SK2.2: Review dashboards, log files, monitoring, system alerts and other security-related information to identify signs of unexpected or anomalous activity SK2.3: Identify security weaknesses within digital systems and explain their potential impact on the confidentiality, integrity and availability of systems, devices and data SK2.4: Apply or recommend appropriate actions that support security improvement, troubleshooting and protection of digital systems SK2.5: Record and organise security-related information clearly and accurately using appropriate digital tools SK2.6: Communicate security concerns, risks and recommended actions clearly for different audiences SK2.7: Escalate potential cyber security concerns using defined workplace procedures SK2.8: Handle security-related information in accordance with privacy, confidentiality and data protection requirements	
Section	**Amplification**
SK2.1 Configure digital systems by applying access controls, authentication requirements, permissions, security settings, secure configuration and update procedures	Learners should be able to configure a defined digital system by: • configuring appropriate authentication, access controls and permissions for relevant users, devices or systems • applying appropriate security settings and protective controls to reduce identified security risks • applying secure configuration settings to meet defined system requirements • applying required system or software updates and patching procedures in line with defined requirements.
SK2.2 Review dashboards, log files, monitoring, system alerts and other security-related information to identify signs of unexpected or anomalous activity	Learners should be able to review security-related information to identify signs of unexpected or anomalous activity by: • using relevant information, such as users, devices, dates, times, actions or status information, to identify unusual activity • comparing recorded activity with expected or authorised activity where appropriate • distinguishing between activity that requires further investigation and activity that is consistent with expected operation.

SK2.3
Identify security weaknesses within digital systems and explain their potential impact on the confidentiality, integrity and availability of systems, devices and data
	Learners should be able to
	• identify security weaknesses by identifying:
	  • weaknesses in access controls and permissions that could allow inappropriate or unauthorised access
	  • weaknesses in authentication measures that could reduce the level of protection provided
	  • unpatched or outdated software that could present a security weakness
	  • system or network settings that do not meet the required secure configuration.

© WJEC CBAC Ltd 2027.

	• explain the potential impact of identified security weaknesses on:
	  • confidentiality of data, devices and systems
	  • integrity of data, devices and systems
	  • availability of data, devices and systems.
	• distinguish between the different impacts where relevant.

SK2.4 Apply or recommend appropriate actions that support security improvement, troubleshooting and protection of digital systems	Learners should be able to: • select appropriate actions to address identified security weaknesses or system issues • apply or recommend changes to access controls, permissions, configuration settings, updates, patching or protective controls, as appropriate • use available system information to support troubleshooting and identify appropriate corrective action.
SK2.5 Record and organise security-related information clearly and accurately using appropriate digital tools	Learners should be able to: • record relevant information about security weaknesses, unexpected activity, actions taken and outcomes • use appropriate technical terminology and include relevant details about the security concern • organise information clearly using appropriate digital tools, headings and labels • review records for accuracy and completeness.
SK2.6 Communicate security concerns, risks and recommended actions clearly for different audiences	Learners should be able to: • describe identified security concerns and risks, including their potential impact and relevant supporting evidence • communicate actions taken or recommended and explain how they address identified concerns or risks • adapt the language, terminology, format and level of technical detail for the intended audience.
SK2.7 Escalate potential cyber security concerns using defined workplace procedures	Learners should be able to: • identify security concerns that require further investigation or escalation • follow a defined procedure to report and escalate security concerns • provide relevant information and evidence to support further investigation • handle security-related information appropriately when escalating a concern.

DRAFT

© WJEC CBAC Ltd 2027.

SK2.8 Handle security-related information in accordance with privacy, confidentiality and data protection requirements	Learners should be able to: • apply appropriate privacy and confidentiality measures when accessing, storing or sharing security-related information • use appropriate access controls and secure methods to protect information from unauthorised access, loss, misuse or disclosure • handle, store, transfer and dispose of security-related information in accordance with defined data protection requirements, including requirements relating to personal data as defined by GDPR and the Data Protection Act 2018 • check that security-related information is handled securely throughout its use.

Transferable skills

LO2	Problem solving	Recording technical information	Communication	Digital capability
SK2.1				✓
SK2.2	✓			✓
SK2.3	✓		✓	✓
SK2.4	✓			✓
SK2.5		✓		✓
SK2.6			✓	
SK2.7		✓	✓	✓
SK2.8				✓

Work-related behaviours

LO2	Responsible	Perceptive	Attention to detail
SK2.1	✓		✓
SK2.2		✓	✓
SK2.3	✓	✓	✓
SK2.4	✓	✓	✓
SK2.5	✓		✓
SK2.6	✓		✓
SK2.7	✓	✓	
SK2.8	✓		✓

© WJEC CBAC Ltd 2027.

LO3 Plan, develop and test a programming solution in order to meet a brief	
Learners will gain skills in the following areas: SK3.1: Plan a programming solution to meet a given brief SK3.2: Develop a programming solution by writing and integrating code SK3.3: Apply a logical, step-by-step approach when developing and refining code SK3.4: Use appropriate software tools to run and test the code within a solution SK3.5: Test the solution to confirm it produces the expected outcome SK3.6: Identify and correct errors in code SK3.7: Communicate outcomes clearly using concise explanations and structured documentation	
Section	**Amplification**
SK3.1 Plan a programming solution to meet a given brief	Learners should be able to plan a programming solution to meet a given brief by: • identifying the purpose, requirements and limitations of the solution • identifying the design elements, inputs, processes and outputs, needed for the solution • breaking down solution design elements into smaller tasks or components and sequencing them • planning algorithms or structured logic for the solution • planning how the solution should be developed, tested and refined.
SK3.2 Develop a programming solution by writing and integrating code	Learners should be able to develop a programming solution by writing and integrating Python code by: • translating planned algorithms and structured logic • using appropriate programming constructs, variables, data types, operators and expressions to implement the solution • using selection and iteration where required to control program behaviour • using clear naming, indentation, comments and structure to make code readable and maintainable • integrating different parts of the solution so that they work together as intended.
SK3.3 Apply a logical, step-by-step approach when developing and refining code	Learners should be able to develop and refine code by: • developing the solution in manageable stages or components • reviewing code and program behaviour as the solution is developed • making appropriate changes to improve the functionality or correctness of the solution • integrate the different parts of the solution so that they work together as intended.
SK3.4 Use appropriate software tools to run and test the code within a solution	Learners should be able to use appropriate software tools to run and test the code by: • using an appropriate development environment or software tool to run Python code • providing inputs and observing the outputs produced • using error messages, warnings or other indicators to identify issues.

© WJEC CBAC Ltd 2027.

SK3.5
Test the solution to confirm it produces the expected outcome
 	
SK3.6
Identify and correct errors in code
	Learners should be able to:
	• test the solution by:
	  • using appropriate test inputs and conditions, including normal, boundary or other relevant conditions where applicable
	  • recording and comparing expected outcomes with actual results
	  • identifying differences between expected and actual behaviour and determining whether the solution meets the requirements of the brief
	  • re-testing the solution following changes or corrections to confirm the expected outcome.
	• identify errors in code using error messages, test results or observed behaviour
	• make appropriate changes to correct identified errors
	• check that corrections resolve the identified errors without adversely affecting other parts of the solution.

SK3.7 Communicate outcomes clearly using concise explanations and structured documentation	Learners should be able to: • choose an appropriate format for the audience • describe the purpose and main functionality of the programming solution • explain how the solution meets the requirements of the brief • summarise relevant development, testing and refinement activities, including significant errors and changes made • record relevant information clearly using appropriate headings, sections and technical terminology • identify any remaining issues or limitations where relevant.

DRAFT

© WJEC CBAC Ltd 2027.

Transferable skills

LO3	Problem solving	Planning and organisation	Communication	Digital capability
SK3.1	✓	✓		✓
SK3.2				✓
SK3.3	✓	✓		✓
SK3.4	✓			✓
SK3.5	✓		✓	✓
SK3.6	✓			✓
SK3.7			✓	✓

Work-related behaviours

LO3	Persistent	Focused	Adaptable
SK3.1		✓	✓
SK3.2	✓	✓	✓
SK3.3	✓	✓	✓
SK3.4	✓	✓	
SK3.5	✓	✓	
SK3.6	✓	✓	✓
SK3.7		✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

LO4 Plan and configure hardware and software components in order to deliver a functional digital system	
Learners will gain skills in the following areas: SK4.1: Plan and sequence tasks and resources to support delivery of a digital system SK4.2: Configure hardware and software components to achieve a functional digital system SK4.3: Verify system operation by checking that components function together as intended SK4.4: Perform routine maintenance activities to support continued operation SK4.5: Record and communicate configuration and maintenance activity clearly to others	
Section	**Amplification**
SK4.1 Plan and sequence tasks and resources to support delivery of a digital system	Learners should be able to plan and sequence tasks to support delivery of a digital system by: • identifying the tasks required to configure and deliver the system • identifying the hardware, software, tools and other resources needed • identifying dependencies between tasks and components • arranging tasks in a logical order, including appropriate checks and review points.
SK4.2 Configure hardware and software components to achieve a functional digital system	Learners should be able to configure hardware and software components to achieve a functional digital system by: • identifying and connecting the hardware components required by the system • installing and configuring the software required to support the intended functionality • configuring relevant hardware and software settings to meet defined requirements • configuring components so that the hardware and software operate together as intended.
SK4.3 Verify system operation by checking that components function together as intended	Learners should be able to verify system operation by: • checking that hardware and software components operate as intended • checking that components interact and communicate correctly • identifying faults, errors or unexpected behaviour affecting system operation • taking appropriate corrective action and repeating checks to confirm that the system operates as intended.
SK4.4 Perform routine maintenance activities to support continued operation	Learners should be able to perform routine maintenance activities by: • carrying out routine actions that help maintain the system in working order • resolving any issues encountered • identifying issues that require further action.

© WJEC CBAC Ltd 2027.

SK4.5 Record and communicate configuration and maintenance activity clearly to others	Learners should be able to: • record configuration and maintenance activities • record relevant issues, actions taken and outcomes • communicate relevant information clearly.

Transferable skills

LO4	Planning and organisation	Problem solving	Recording info	Communication	Digital capability
SK4.1	✓				✓
SK4.2	✓	✓			✓
SK4.3		✓			✓
SK4.4		✓			✓
SK4.5			✓	✓	✓

Work-related behaviours

LO4	Organised	Flexible	Committed
SK4.1	✓	✓	✓
SK4.2	✓	✓	✓
SK4.3		✓	✓
SK4.4	✓	✓	✓
SK4.5	✓	✓	

DRAFT

© WJEC CBAC Ltd 2027.

3. Assessment

Assessment support materials will include all detailed information relating to assessment.

3.1. Assessment overview

Assessment 1

Content Area 1 is assessed through an externally set and marked examination.
The assessment must be taken under invigilated examination conditions in accordance with JCQ requirements (see http://www.jcq.org.uk/exams-office/ice---instructions-for-conducting-examinations).

This assessment is externally set and marked by WJEC.

Assessment 2

This is assessed through an externally set non-exam assessment, which is marked by the centre and externally moderated by WJEC. Learners are required to complete a series of tasks based on an externally brief.

A new brief will be issued annually through Portal during the third week of March with the assessment window ending on 1 May of that academic year. Learners must not have access to the brief or associated tasks until the start of the assessment window. Centres have the flexibility to schedule the assessment at any point during the assessment window.

Assessment sessions may be arranged across multiple sittings within an 18-day window, allowing learners to undertake the practical and applied tasks in a manageable manner while generating the evidence required for assessment.

The assessment must be submitted digitally, either as scanned handwritten responses or completed electronically or as audio/visual evidence.

Assessment 3

This is assessed through an externally set non-exam assessment, which is marked by the centre and externally moderated by WJEC. Learners are required to complete a series of tasks based on an externally set brief.

A new brief will be issued annually through Portal during the first week of March for use within that academic year. Learners must not have access to the brief or associated tasks until the start of the assessment. Centres have the flexibility to schedule the assessment at any point during the academic year.

Assessment sessions may be arranged across multiple sittings within a 28-day window, allowing learners to undertake the practical and applied tasks in a manageable manner while generating the evidence required for assessment.

The assessment must be submitted digitally, either as scanned handwritten responses or completed electronically or as audio/visual evidence.

© WJEC CBAC Ltd 2027.

The Assessment 2 and 3 briefs these will be written to cover one of these digital subsectors:

- business intelligence and digital transformation
- cyber security
- data and analytics
- IT infrastructure and operations
- software and systems development.

The two briefs used in an assessment series will each choose a different subsector.

3.2. Synoptic assessment

The non-exam content areas are synoptic in that the LO skills covered are underpinned by the corresponding LO knowledge and understanding.

DRAFT

© WJEC CBAC Ltd 2027.

4. Technical information

4.1. Assessment availability

Assessment	Winter Yr-1	Summer Yr-1
Foundations of Digital Systems and Data Assessment 1	✓	✓
Digital Data and Sources in Practice Assessment 2	×	✓
Digital Systems in Practice Assessment 3	×	✓

4.2. Assessment entries

You must enter candidates for each assessment they wish to take. Entry for assessments must be made using the entry code below.

	Entry code
Content Area 1	
Content Area 2	
Content Area 3	

If a candidate has been entered for but is absent for an assessment, the absence does not count as an attempt.

4.3. Claiming the qualification

Once candidates have completed all their assessments, you must claim their qualification using the cash-in code below.

Claiming the qualification and entering the cash-in code enables aggregation to take place, grades to be calculated, and results to be issued.

Cash-in code	

The current edition of our Entry Procedures and Coding Information gives up-to-date entry procedures.

4.4. Assessment reporting

Foundation Certificate qualifications and the assessments within them are reported on a three-point scale: Distinction, Merit and Pass. Learners who do not achieve the minimum standard required for a Pass will be awarded an Unclassified result.

© WJEC CBAC Ltd 2027.

DRAFT

Individual assessment results are reported on a uniform mark scale (UMS) with the following grade equivalences:

	Max.	Distinction	Merit	Pass
Content Area 1	100	80	60	40
Content Area 2	60	48	36	24
Content Area 3	90	72	54	36

The uniform marks obtained for each assessment are added up and the qualification grade is based on this total.

	Max.	Distinction	Merit	Pass
Qualification	250	200	150	100

Candidates who do not achieve the uniform marks required to achieve a Pass will have their achievement recorded as U (unclassified) and will not receive a certificate.

DRAFT

© WJEC CBAC Ltd 2027.

Appendix A – Glossary of terms

Term	Definition
Access control	The methods and rules used to determine which users, devices or systems are permitted to access data, systems or services, and the level of access they are allowed.
Access permission	A setting that controls which users, devices or systems are allowed to view, use or modify specific data, systems or services.
Acceptable use policies	Rules for appropriate use of systems, networks and devices provided by an organisation.
Algorithm	A defined sequence of instructions that a computer follows to process inputs and produce an output or solve a problem.
Anomalous activity	Any action, behaviour, or event that is unusual, unexpected, or differs from what is considered normal within a system, process, or environment.
Artificial intelligence (AI)	Digital systems or tools that analyse data using algorithms or models in order to generate outputs such as predictions, insights, classifications or recommendations.
Attribution (IPR)	The acknowledgement of the original creator, owner, or source of a piece of intellectual property when it is used, shared, or reproduced. Attribution typically involves clearly identifying who created the work to recognise their ownership and contribution and to comply with any legal or licensing requirements.
Authentication	A security process used to confirm the identity of a user, device or system before access to data, systems or services is granted.
Automated and AI-enabled systems	Digital tools or systems that use automated processes, artificial intelligence or both to generate, support or refine outputs.
Automation	The use of programmed instructions or scripts that allow digital systems to perform tasks or processes automatically with limited human intervention.
Availability	The condition in which information, systems or services are accessible and usable by authorised users when required.
Bias	A tendency within information that can influence how it is presented, interpreted or used.
Black box testing	A method of testing a system, application, or product by checking its inputs and outputs without examining its internal code, structure, or how it works.
Brief	A statement that defines a task, including its purpose, requirements, constraints and intended outcome.

© WJEC CBAC Ltd 2027.

Term	Definition
Central Processing Unit (CPU)	The main processor in a computer that carries out instructions, performs calculations, and controls the operation of other hardware and software.
Chart	A graphical representation of data used to show patterns, comparisons or relationships between values.
Code	Instructions written in a programming or scripting language that tell a computer how to perform specific tasks or operations.
Component	A hardware or software element that forms part of a larger digital system and contributes to its operation.
Component compatibility	The ability of hardware, software or other digital system components to operate together as intended.
Confidentiality	The protection of information so that it is only accessible to authorised users and is not disclosed to unauthorised individuals or systems.
Configuration	The process of setting or adjusting parameters in hardware or software so that a system operates correctly and securely for its intended purpose.
Control (security control)	A measure, safeguard or procedure designed to reduce risks to systems, services or data.
Cyber security	The practice of protecting computers, networks, systems, and data from unauthorised access, attacks, damage, or theft.
Dashboard	A visual display that brings together important information, data, and performance measures in one place so they can be monitored and understood quickly
Database	An organised collection of data that is stored electronically so that it can be easily accessed, managed, updated, and searched. Data is typically organised into fields (individual pieces of information, such as a name or date) and records (a complete set of related fields describing a single item, person, or event).
Dataset	A structured collection of related data items organised so that they can be stored, processed, analysed or presented.
Data protection	The practice of keeping personal data safe and ensuring it is collected, stored, used, and shared lawfully and securely. In the UK the Data Protection Act 2018 sets out the rules that organisations must follow when processing personal data and gives individuals rights over how their personal information is used.

DRAFT

© WJEC CBAC Ltd 2027.

Term	Definition
Data types	Categories that describe the kind of data being stored, processed, or used in a digital system. Categorial data that is grouped into categories or labels rather than measured numerically. The values represent characteristics, qualities, or types and are used to classify items into distinct groups. There is: • nominal – data with no natural order or ranking • ordinal – data with meaningful order or ranking. Standard data types are: • Boolean – a categorical logical data type that contains one of two values only: TRUE or FALSE • currency – a numeric data format used to represent monetary values • date and time – a value representing a date, a time, or both. Formatted for readability and use in calculations • integer – a whole number value that can be used in calculations • float – a numeric data type that can store decimal/fractional values • percentage – a numeric value expressed as a fraction of 100 • text – a sequence of characters not required for use in calculations.
Dependency	A relationship in which one component, process or service relies on another in order to function correctly.
Digital devices	Electronic devices that use digital technology to process, store, transmit, or display data such as computers, smartphones, tablets.
Digital information	Data that is stored, processed, or transmitted in a digital format that can be understood and used by computers and other digital devices.
Digital network	A group of connected devices and infrastructure that communicate with each other to exchange data and provide access to digital services.
Digital services	Services that are delivered, accessed, or used through digital technologies such as the internet, computers, mobile devices, or online platforms such as cloud storage, email services.
Digital solutions	Digital tools, systems, or applications that are used to solve problems, improve processes, or meet user needs.

© WJEC CBAC Ltd 2027.

Term	Definition
Digital system	A set of connected components, including hardware, software, data, networks and users, which work together to deliver a digital function or service. The system also issues alerts, either a message or notification generated by a computer system to inform users about an event, condition, error, warning, or action that requires attention.
Digital tool	Software, application or digital feature used to support the completion of a task.
Error	A mistake or fault in code, data or configuration that causes a system or program to produce an incorrect or unexpected result.
Functional	Operating correctly and producing the intended result for a designed purpose.
General Data Protection Regulation (GDPR)	A law that protects people's personal data and gives them rights over how their information is collected, used, stored, and shared. It works alongside the Data Protection Act 2018 to ensure that personal data is processed securely and that individuals' privacy rights are protected.
HyperText Transfer Protocol (HTTP)/HyperText Transfer Protocol Secure (HTTPS)	A set of rules that allows web browsers and web servers to communicate and transfer information over the internet. HTTPs is a secure version of HTTP that encrypts data sent between a web browser and a web server to help protect information from being intercepted or accessed by unauthorised users.
Hallucinated output	Information generated by an automated or AI-enabled system that is inaccurate, misleading or fabricated.
Hardware	The physical parts of a computer or digital device that can be seen and touched such as CPU, hard drive, keyboard, monitor, mouse, printer.
Internet Protocol (IP)	A set of rules used to identify devices and transfer data across networks, including the internet.
Incorrect conditions	Circumstances, settings, or requirements that are unsuitable, inappropriate, or not set up properly for a task, process, or system to operate as intended.
Infrastructure components	Physical and virtual resources that support the operation of computer systems, networks, and digital services.
Integrity	The accuracy, completeness and reliability of data, ensuring that information has not been altered in an unauthorised way.
Intellectual property rights (IPR)	Legal rights that protect creations of the mind, giving creators ownership and control over how their work is used by others for example, copyright protecting a software program.

DRAFT

© WJEC CBAC Ltd 2027.

Term	Definition
Local area networks (LANs)	A network that connects computers, devices and resources within a limited geographical area, such as a home, office or school.
Log files	Records that automatically store information about events, activities, or actions that occur within a computer system, application, or network.
Logical	Based on clear and ordered reasoning in which steps follow a defined and consistent sequence.
Message Queuing Telemetry Transport (MQTT)	A lightweight communication protocol that allows devices to send and receive messages over a network.
Maintenance	Activities such as updates, checks, repairs or adjustments carried out to ensure that systems continue to operate effectively.
Online data repository	A storage location on the internet where digital data can be securely stored, organised, managed, and accessed by authorised users.
Portable Appliance Testing (PAT)	The process of inspecting and testing electrical appliances to help ensure they are safe to use.
Patched software	Software has had updates (known as patches) applied to fix bugs, close security vulnerabilities, improve performance, or add minor improvements, helping the software remain secure and function correctly.
Pattern	A repeated or noticeable relationship or trend within data.
Passphrase	A sequence of words used to verify identity and allow secure access to a system, device or service.
Protocol	A defined set of rules that governs how data is transmitted and received between devices or systems.
Program	A complete set of code that performs a specific function or set of tasks when executed by a computer.
Programming	The process of designing, writing, testing and refining code to create a digital solution that meets a defined purpose.
Random Access Memory (RAM)	A type of computer memory that temporarily stores data and instructions that are currently being used by the computer.
Recommendation	A proposed course of action that is supported by analysis, evidence or evaluation.
Reliability (of a source)	The degree to which information from a source can be trusted as accurate, credible and appropriate for the intended purpose.
Risk	The possibility that an event or action may cause harm, loss or disruption to systems, data or services.

© WJEC CBAC Ltd 2027.

Term	Definition
Secure handling	Managing data, devices or systems in ways that prevent unauthorised access, loss, misuse or disclosure.
Security weakness	A flaw, vulnerability, or weakness in a system, network, device, or process that could be exploited to gain unauthorised access, cause damage, or compromise data.
Sequencing	Arranging tasks, instructions or steps in the correct logical order so that a process operates as intended.
Simulated environment	A digital environment that replicates the features or functionality of a real digital system for the purposes of configuration, testing or maintenance.
Software	A collection of programs, instructions, and data that tell a computer or digital device how to perform specific tasks for example, antivirus software, operating system such as Windows, web browsers.
Source (digital source)	A location from which information, data or code is obtained.
Survey output	The information, results, or findings produced from collecting and analysing responses to a survey.
Syntax errors	Mistakes in the rules or structure of code that prevent a program from being interpreted or run correctly, such as missing a closing bracket, forgetting a quotation mark, misspelling a command or keyword.
System generated report	A report that is automatically created by a computer system or software using data it has collected or processed.
Troubleshooting	The process of identifying, investigating, and resolving problems or faults in a system, device, software application, or network.
Transmission Control Protocol (TCP)	A communication protocol that enables reliable data transfer between devices over a network.
Test	An activity carried out to check whether a system, program or component behaves as expected.
Unpatched software	This has not had the latest updates or patches applied, meaning it may contain known bugs, security vulnerabilities, or performance issues that could affect its reliability and security.
Updates	Changes, improvements, or fixes made to software, systems, or devices to improve performance, add new features, or address security issues.
User interface (UI) elements	The visual and interactive components of a digital system that allow users to interact with software, applications, or websites such as buttons, icons, menus, text boxes.
Values	Pieces of data or information that are stored, entered, or processed within a computer system, program, or database.

DRAFT

© WJEC CBAC Ltd 2027.

Term	Definition
Verification	The process of checking that data, information, or a system is accurate, complete, and meets the required specifications or requirements.
Vulnerability	A weakness in a system, configuration, process or control that could be exploited to compromise security, functionality or reliability.
Visualise	To present information or data in graphical or pictorial form to support interpretation and understanding.
White box testing	A method of testing software by examining and testing its internal code, structure, and logic to ensure it works correctly.
Wide area networks (WANs)	A network that connects computers, devices, or smaller networks across large geographical areas, such as cities, countries, or the world.

DRAFT

© WJEC CBAC Ltd 2027.

Appendix B – Minimum delivery requirements/resources

These are the minimum requirements and resources that centres would need to have to deliver this qualification.

Digital devices	Centres must provide learners with access to: • desktop or laptop computers capable of running spreadsheet, programming and system configuration software • access to individual devices during supervised assessment activities • internet-enabled devices for research and access to digital information sources when permitted • appropriate digital storage for learner work and assessment evidence. For Assessment 2 each candidate machine to have at least 8 GB of memory, 30 GB of free disk space, and virtualisation switched on.
Software	Centres must provide access to tools for data analysis and presentation: • spreadsheet software capable of sorting, filtering, formatting and analysing datasets • software capable of producing charts, tables and visual representations of data • document production software for reports and recommendations.
Programming software	• Version Python 3 or newer • A Python-compatible development environment (IDE) • Software that allows learners to create, run, test and debug Python programs
Hardware	Physical hardware may be supplemented by virtualised or simulated environments where appropriate. Centres must provide opportunities for learners to work with hardware components and peripheral devices, including: • computers and associated peripherals (where appropriate) • wired and wireless network connectivity • storage devices • printers or other peripheral devices where appropriate for configuration activities. For Assessment 2 they will need: • a school server (the host) with at least 8 GB of memory (16 GB or more if several VMs will run on it at once), at least 50 GB of free disk space, and a recent 64-bit processor • administrator access to the server and to each candidate machine • a way to move a large file to each candidate machine, such as a network share, an external drive or a USB drive of at least 16 GB.

© WJEC CBAC Ltd 2027.

Virtual environments	Suitable environments may include: • virtual machines, such as VirtualBox or similar virtualisation software, Microsoft Hyper-V, VMware Workstation • educational network simulators • cloud-based simulation environments. They must allow learners to: • manage individual user accounts and role-based folder permissions • configure password/sign-in settings, screen lock and MFA (or an equivalent simulated control) • view and change firewall and update status • review sign-in, permission-change and export logs • record configuration changes and verify the outcome • submit an incident report using a restricted or simulated secure reporting route. Any can be used for teaching and learning; however, some Content Area 3 tasks **must** be done on VirtualBox.
Data resources	Centres must provide access to: • structured datasets in CSV format • datasets containing realistic data quality issues such as missing values, duplicate records and inconsistent formatting • digital information sources suitable for research and evaluation activities • examples of organisational policies, procedures and system documentation where required.
Network and internet access	Centres must provide: • reliable internet access • access to online digital sources and repositories • access to locally networked or simulated networked environments to support delivery of networking and security concepts.
Assessment evidence	Centres must be able to support the collection and storage of assessment evidence, including: • electronic documents • spreadsheets • program code files • screenshots • system logs or configuration records • audio or video evidence where permitted by assessment requirements.

© WJEC CBAC Ltd 2027.

Appendix C – Transferable skills

Through the five learning outcomes, learners will develop transferable skills, including:

- planning – structured activities such as cleaning datasets, developing code, configuring systems and delivering digital systems by identifying steps, sequencing tasks, estimating resources and managing time
- data interpretation – data, systems and digital scenarios by organising information into types, identifying patterns and anomalies, deconstructing problems, and understanding how components interact
- problem solving – evaluating information, data, systems behaviour and AI-enabled outputs by questioning accuracy, weighing pros and cons, applying logical reasoning and reaching justified conclusions
- communicating – findings, risks and recommendations clearly using written, visual and digital formats, adapting explanations and terminology to suit purpose and audience
- investigating –suitable digital sources, interrogating datasets, reviewing logs and dashboards, and designing and carrying out tests to confirm accuracy, function or security
- evidence-based decision-making – when selecting tools, configurations and solutions, assessing likely impact, and justifying recommended actions or improvements
- self-managing – own performance by working through multi-stage tasks, monitoring progress, checking accuracy, responding to feedback and refining outcomes through testing and review
- recording – information accurately by capturing, storing and organising digital content such as datasets, code, configurations, findings and documentation
- evaluating – processes, evidence and outcomes by reviewing effectiveness, appraising accuracy and reliability, and making recommendations for improvement
- observing – situational awareness by monitoring system outputs, data quality, error messages, logs and alerts to identify issues or abnormal behaviour.

This provides more detail for each LO about the transferable skills to be developed and demonstrated.

LO1

Transferable skills to be developed and demonstrated through this learning outcome include:

- analytical reasoning when identifying patterns and checking data accuracy
- recording information clearly when preparing data and presenting outputs
- clear communication when presenting findings through tables, charts and written explanations
- numeracy in interpreting totals, averages and proportions within datasets
- digital capability in manipulating and presenting data using appropriate tools.

LO2

Transferable skills to be developed and demonstrated through this learning outcome, include:

- problem solving when identifying security weaknesses and applying appropriate protective measures
- recording technical information clearly using structured digital documentation
- communication when explaining security risks and recommended actions
- digital capability in configuring digital systems and using digital tools to monitor and review security information.

© WJEC CBAC Ltd 2027.

LO3
Transferable skills to be developed and demonstrated through this learning outcome, include:

- problem solving when identifying errors and refining programming solutions
- planning and organisation when structuring and developing programming solutions
- communication in explaining solution behaviour and testing outcomes
- digital capability in developing, running and testing program code.

LO4
Transferable skills to be developed and demonstrated through this learning outcome, include:

- planning and organisation in sequencing tasks and managing resources to deliver a digital system
- problem solving when identifying faults and adjusting configurations
- recording information accurately when documenting configuration and maintenance activity
- digital capability in integrating hardware and software components to achieve a functional system.

LO5
Transferable skills to be developed and demonstrated through this learning outcome, include:

- research skills in locating and selecting relevant digital information
- analytical reasoning when comparing information across sources to support conclusions
- communication in presenting evidence-based recommendations clearly
- digital capability in organising information and referencing sources appropriately.

DRAFT

© WJEC CBAC Ltd 2027.

Appendix D – Mapping to Level 3 qualifications

The Level 2 Foundation Certificate content introduces foundational concepts and practices. Progression is characterised by increased complexity, independence and specialisation, moving from routine applications at Level 2 to occupationally relevant technical practice at Level 3.

Learners progress from structured, clearly defined tasks at Level 2, to more independent work at Level 3, typically requiring learners to interpret requirements, use judgement for informed decision-making and respond to a broader range of defined work-related contexts.

Link to V Levels

The following aspects of this Foundation Certificate content directly relate to content specified in the V Level Digital Systems and Data, to provide a stepping-stone and clear line of sight from level 2 to level 3 study:

Foundation Certificate reference	V Level reference	Knowledge and understanding	Skills
LO1: Data types and structured datasets	WRP1	Data structure, format, field definitions and levels of detail associated with datasets obtained from different sources.	Preparing datasets for analysis.
LO1: Data quality and preparation	WRP1	Data quality issues including missing data, duplicates and inconsistent formatting and their impact on analysis.	Validating and preparing datasets.
LO1: Data analysis methods	WRP1	Analytical techniques including sorting, filtering, grouping, calculating totals, averages and identifying trends.	Analysing data and identifying patterns.
LO1: Data presentation	WRP1	Forms and uses of analytical outputs and principles of visual communication.	Presenting analytical findings clearly.
LO2: Digital system configuration	Core KU/WRP3	Configuration requirements relating to connectivity, storage, security settings and system behaviour.	Preparing, configuring and testing digital systems.
LO2: Authentication and access control	WRP2	Authentication requirements, access controls, user permissions and data protection measures.	Applying security protocols and configuration controls.

© WJEC CBAC Ltd 2027.

Foundation Certificate reference	V Level reference	Knowledge and understanding	Skills
LO2: Security weaknesses, risks and vulnerabilities	Core KU/WRP2	Indicators of cyber security concerns, configuration related risks and system vulnerabilities.	Reviewing system information, identifying risks and responding appropriately.
LO2: Security impact and protective actions	WRP2	Implications of cyber threats, system vulnerabilities and delayed identification.	Applying protective actions and security procedures.
LO2: Security reporting and escalation	WRP2	Policies and procedures relating to incident reporting, privacy, confidentiality and secure handling of information.	Recording, communicating and escalating security concerns.
LO3: Algorithms and structured logic	WRP4	Principles of algorithms and structured coding approaches.	Structuring digital solutions using logical steps.
LO3: Program development	WRP4	Relationship between algorithms, program code and outputs.	Developing programming solutions using code.
LO3: Testing programming solutions	WRP4 and Core KU	Purpose of testing digital systems and role of quality assurance.	Testing and refining solutions and evaluating readiness.
LO4: Hardware and software interaction	Core KU	Relationship between system components and system behaviour.	Configuring system components to deliver functionality.
LO4: System testing and readiness	Core KU	Relationship between requirements, test outcomes and system readiness.	Verifying system performance and readiness.
LO4: Technical fault identification	Core KU	Nature and causes of technical faults and structured diagnostic approaches.	Diagnosing faults and troubleshooting systems.
LO5: Reliability of digital information	WRP1	Data limitations, bias and reliability of datasets and sources.	Evaluating information sources.

DRAFT

© WJEC CBAC Ltd 2027.

Foundation Certificate reference	V Level reference	Knowledge and understanding	Skills
LO5: Evidence-based conclusions	WRP1	Relationship between analysis, data quality and confidence in conclusions.	Drawing justified conclusions.
LO5: Communication of evidence	Core KU	Communication principles in technical and digital contexts.	Presenting evidence-based recommendations.
LO5: Collaborative interpretation	Core KU	Role of collaboration and shared understanding in interpreting information.	Supporting decision making through shared analysis.

DRAFT

© WJEC CBAC Ltd 2027.

Link to T Levels

The Foundation Certificate prepares learners for progression to multiple T Level qualifications including Digital Software Development, Digital Support and Security, and Digital Data Analytics, which builds on and extends into specialised technical knowledge and workplace application leading to roles in software development, cyber security, IT support and data analysis.

The following aspects of this Foundation Certificate content directly relate to content specified in the T Levels Digital systems and intelligence qualifications 'core' content, to provide a stepping-stone and clear line of sight from level 2 to level 3 study:

Foundation Certificate reference	T Level reference	Knowledge and understanding	Skills
LO1: Clean, interpret and visualise a dataset	Digital Data Analytics – Data preparation and analysis	Data types, structured datasets and data quality issues.	Preparing and validating datasets.
LO1: Clean, interpret and visualise a dataset	Digital Data Analytics – Data analysis and visualisation	Analytical techniques for identifying patterns and trends in data.	Analysing datasets and interpreting outputs.
LO1: Clean, interpret and visualise a dataset	Digital Data Analytics – Communication of insights	Use of charts, tables and summaries to communicate findings.	Presenting findings and insights to technical and non-technical audiences.
LO2: Configure and secure digital systems	Digital Support and Security – Digital environments and systems	Components of digital systems including devices, networks and software.	Configuring digital systems and connectivity.
LO2: Configure and secure digital systems	Digital Support and Security – Security protocols	Authentication methods, access permissions and secure configuration.	Applying security controls and monitoring system behaviour.
LO2: Configure and secure digital systems	Digital Support and Security – Cyber security awareness	Indicators of vulnerabilities or suspicious activity in digital systems.	Identifying and responding to potential security risks.
LO2: Configure and secure digital systems	Digital Support and Security – Cyber security monitoring	Monitoring system activity to identify security weaknesses, vulnerabilities and anomalous behaviour	Reviewing system activity to identify weaknesses and risks.
LO2: Configure and secure digital systems	Digital Support and Security – Security procedures and escalation	Policies and procedures relating to privacy, confidentiality and incident reporting.	Recording, communicating and escalating cyber security concerns.

© WJEC CBAC Ltd 2027.

Foundation Certificate reference	T Level reference	Knowledge and understanding	Skills
LO3: Plan, develop and test a programming solution	Digital Software Development – Programming and problem solving	Algorithms, structured logic and program design.	Structuring digital solutions and writing code.
LO3: Plan, develop and test a programming solution	Digital Software Development – Software development lifecycle	Planning, developing and testing coded solutions.	Developing and testing digital solutions.
LO4: Configure hardware and software to deliver a functional digital system	Digital Support and Security – System configuration and testing	Interaction between hardware, software and network components.	Configuring and testing digital systems.
LO4: Configure hardware and software to deliver a functional digital system	Digital Support and Security – Fault identification and system reliability	Technical faults affecting digital systems and diagnostic processes.	Troubleshooting and verifying system performance.
LO5: Select and apply reliable digital sources	Digital Data Analytics – Data reliability and governance	Reliability, bias and limitations of digital information and datasets.	Evaluating information sources.
LO5: Select and apply reliable digital sources	Digital Software Development / Data Analytics – Decision making using digital information	Relationship between data, evidence and decision-making.	Communicating evidence-based conclusions.

DRAFT

© WJEC CBAC Ltd 2027.

Link to A Levels

The Foundation Certificate prepares learners for progression to A Level in Computer Science, which extends into advanced level 3 topics not covered at Level 2, including algorithm efficiency, formal data structures, programming paradigms, Boolean algebra or database design, which provides clear differentiation between level 2 and A Level study.

The following aspects of this Foundation Certificate content directly relate to content specified in the A Level computer science qualification, to provide a stepping-stone and clear line of sight from level 2 to level 3 study:

Foundation Certificate reference	A Level reference	Knowledge and understanding	Skills
LO1: Data cleaning and visualisation	Data representation	Data types: numerical, categorical, text and date/time data.	Interpreting datasets; recognising patterns; applying numeracy in digital contexts.
LO1: Data cleaning and visualisation	Data management	Methods of capturing, selecting and managing data to produce information.	Organising and preparing datasets for analysis.
LO1: Data cleaning and visualisation	Computational thinking	Interpreting patterns and relationships in data.	Analytical reasoning; drawing conclusions from data.
LO1: Data cleaning and visualisation	Communication of information	Presenting data using tables and charts.	Communicating findings clearly using visual and written formats.
LO2: Networks and security configuration	Computer systems architecture	Role of devices, infrastructure components and software in digital networks.	Configuring digital systems and devices.
LO2: Networks and security configuration	Networks and protocols	Characteristics of networks and the role of communication protocols.	Understanding system connectivity and communication.
LO2: Networks and security configuration	Cybersecurity fundamentals	Confidentiality, integrity and availability of data and services.	Identifying risks and applying security controls.
LO3: Planning, developing and testing a programming solution	Fundamentals of programming	Relationship between algorithms, program code and solution outputs.	Designing program logic and structured solutions.

© WJEC CBAC Ltd 2027.

Foundation Certificate reference	A Level reference	Knowledge and understanding	Skills
LO3: Planning, developing and testing a programming solution	Algorithms	Algorithms as ordered instructions to solve problems.	Computational problem solving and logical reasoning.
LO3: Planning, developing and testing a programming solution	Program development	Debugging and correcting syntax and logic errors.	Testing and refining code.
LO3: Planning, developing and testing a programming solution	Software development process	Planning, writing and testing a coded solution.	Applying structured development processes.
LO4: Configuring hardware and software systems	Computer systems	Interaction between hardware and software components.	Configuring systems to achieve a functional and efficient digital system.
LO5: Evidence-based recommendations	Computational thinking and problem solving	Reliability, bias and evaluation of information.	Evaluating evidence and justifying conclusions.

DRAFT

© WJEC CBAC Ltd 2027.