eduqas

LEVEL 3 V LEVEL

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 3 V Level Digital Systems and Data
Qualification objective	The WJEC V Level in Digital Systems and Data provides learners with the knowledge, understanding and skills associated with a broad vocational area. The qualification supports progression to higher education, higher technical training and apprenticeships 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 higher education providers, training providers and employers.
WJEC Qualification Code	TBC
QAN Number	TBC
Age groups approved for	16–19, 19+
First teaching	September 2027
First certification	Summer 2029

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.

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

- V Level Qualification Level Conditions and Requirements, which set out the regulatory requirements that apply to all V Level qualifications.
- V Level Qualification Level Guidance, which supports compliance with the V Level Qualification Level Conditions and Requirements.
- V Level Subject Level Conditions and requirements for digital systems and data , which set out the additional requirements specific to this V Level subject.

© WJEC CBAC Ltd 2027.

DRAFT

- Guidance in relation to the assessment objectives for V Levels in digital systems and data, which provides requirements and guidance relating to assessment objectives.
- 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 V Levels 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 9
1.3. Guided Learning Hours (GLH) and Total Qualification Time (TQT) 9
1.4. Use of language 10
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
2.4 Synoptic links 12
Content Area 1 Fundamentals of Digital Systems and Data 13
Content Area 2 Data Analysis and Insights 38
3. Assessment 96
3.1. Assessment objectives and weightings 96
3.2. Assessment overview 96
4. Technical information 99
4.1. Assessment availability 99
4.2. Assessment entries 99
4.3. Claiming the qualification 100
4.4. Grading and reporting 100
Appendix A – Glossary of terms 101
Appendix B – Minimum delivery requirements/resources 105
Appendix C – Links to Occupational Standards 107
Appendix D – Links to Digital Systems and Data Foundation Certificate 108

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

All learners must complete the following assessments:			
Content Area	**Assessment**	**Weighting**	**Marks**
Content Area 1: Fundamentals of Digital Systems and Data	**Assessment 1:** Assessment by examination: 1 hour 30 minutes On-screen only	20% of qualification	80 marks
	Assessment 2: Assessment by examination: 2 hours On-screen only	20% of qualification	80 marks
Content Area 2: Data Analysis and Insights	**Assessment 3:** Non-exam assessment: 20 hours	20% of qualification	80 marks
Content Area 3: Cyber Security and Secure Digital Systems	**Assessment 4:** Non-exam assessment: 18 hours	20% of qualification	80 marks

Learners will complete one of the following assessments depending on the content area selected:			
Content Area	**Assessment**	**Weighting**	**Marks**
Content Area 4: Digital Systems Configuration, Testing and Support (Optional route)	**Assessment 5a:** Non-exam assessment: 15 hours	20% of qualification	80 marks
Content Area 5: Digital Solution Design and Development (Optional route)	**Assessment 5b:** Non-exam assessment: 15 hours	20% of qualification	80 marks

Click here to enter accreditation number.

© WJEC CBAC Ltd 2027.

1. Introduction

1.1. Purpose and aims

WJEC V Levels are Level 3 qualifications designed for learners aged 16 to 19 who wish to develop knowledge, understanding and skills within a broad vocational area while keeping their future progression options open.

The qualifications provide 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 progression to further study, training and employment.

V Levels are intended primarily to support progression to higher education, higher technical qualifications, apprenticeships and other forms of post-18 study and training. They enable learners to explore a vocational sector in depth, helping them make informed decisions about their future learning and career pathways.

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

WJEC V Levels:

- 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
- support progression to higher education, higher technical qualifications, apprenticeships and other forms of post-18 study and training
- develop transferable skills and behaviours valued in further learning and employment
- provide valid and reliable evidence of learner attainment
- support universities, training providers and employers in making progression and selection decisions
- help learners make informed choices about future study, training and employment opportunities

This qualification is aligned with Level 3 of the Regulated Qualifications Framework (RQF) and forms part of the V Level qualification suite regulated by Ofqual.

The aims and purpose of the V Level in Digital Systems and Data is to enable learners to:
Apply their knowledge, skills and understanding to achieve the following work related purposes (WRP):

- WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making
- WRP2: Apply security protocols and interpret system information to detect and escalate cyber security concerns
- WRP3: Prepare, configure and assure readiness of digital systems to meet user needs (optional)
- WRP4: Design and create a digital solution to meet defined user needs (optional).

DRAFT

© WJEC CBAC Ltd 2027.

Through this, develop transferable skills, including:

- critical, analytical and logical thinking
- problem solving and decision making
- communication
- collaboration.

Develop in-depth knowledge and understanding of the key theories and principles which support effective practice in the subject, including:

- digital systems and their components
- data and information and their analysis
- cyber security principles
- system configuration and testing
- principles of problem solving and solution design
- usability and accessibility
- ethical and responsible use of digital technologies.

DRAFT

© WJEC CBAC Ltd 2027.

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 are ready to undertake study at Level 3.

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

The qualification is intended primarily to support progression to higher education, higher and degree apprenticeships, higher technical qualifications and other forms of post-18 study and training, where appropriate. It provides a broad foundation for further learning by enabling learners to develop and demonstrate knowledge, understanding and skills within a vocational area.

Achievement in the qualification can support progression and selection decisions by higher education providers, training providers and employers, helping learners make informed choices about their future education, training and career pathways.

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

V Level Digital Systems and Data has been designed to be delivered within 360 guided learning hours. The qualification has been designed as a 2-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	33.33%	120
Content Area 2	22.22%	80
Content Area 3	22.22%	80
Content Area 4 (optional)	22.22%	80
Content Area 5 (optional)	22.22%	80
Totals	**100%**	**360 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.

© WJEC CBAC Ltd 2027.

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, and
- 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 600 hours. This includes:

- 360 hours of guided learning and/or supervised assessment
- 240 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.

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 systems and data 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.

© WJEC CBAC Ltd 2027.

DRAFT

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.
Topics	Lists the topics learners will study as part of the content.
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 stems to indicate the expected depth of learning.

'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.

'Learners should be able to' is used when learners are expected to use their knowledge and understanding in practical or authentic situations or demonstrate application of practical skills and techniques.

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.

DRAFT

© WJEC CBAC Ltd 2027.

2.4 Synoptic links

Throughout the qualification, learners are expected to draw together and apply knowledge, understanding and skills from across different content areas when responding to activities, scenarios and tasks within a range of educational contexts. The synoptic links are identified within each content area.

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 1 Fundamentals of Digital Systems and Data

GLH	120
Overview of content area	This content area develops the knowledge and understanding that underpin effective digital practice. Learners explore how digital systems are designed, configured, maintained and improved to meet user and organisational needs. They develop an understanding of how digital professionals support users, solve problems, collaborate with others, create digital solutions and apply emerging technologies responsibly. The content area provides the conceptual foundation for the qualification, supporting learners to develop a coherent understanding of digital technologies, professional practice and the wider digital environment. It introduces the key principles, concepts and approaches that underpin achievement across the qualification's work-related purposes. Where concepts are reflected across both Content Area 1 and Content Areas 2-5, this content area defines the knowledge and understanding that learners are expected to acquire. Content Areas 2-5 then provide opportunities for learners to apply, demonstrate and extend that understanding in authentic vocational contexts. Learners are expected to draw upon and further develop this knowledge throughout the qualification as they engage with the activities, scenarios and tasks contained within the work-related purposes.
Topics	1.1 Digital systems fundamentals 1.2 System configuration and administration 1.3 Testing and system readiness 1.4 Fault diagnosis and technical support 1.5 Communication and user support 1.6 Collaboration and requirements Analysis 1.7 Digital systems design and development 1.8 AI, Ethics and responsible digital practice
Summary of assessment	Assessment by examination (On-screen only) Assessment 1: Fundamentals of Digital Systems and Data 1 • 1 hour 30 minutes • Set and marked by WJEC • 80 marks. Assessment 2: Fundamentals of Digital Systems and Data 2 – Case Study • 2 hours • Set and marked by WJEC • 80 marks.
Resources required for assessment	Access to digital devices and Surpass software.

© WJEC CBAC Ltd 2027.

Content

1.1 Digital systems fundamentals

This topic introduces the fundamental components and operation of digital systems. Learners develop knowledge and understanding of how hardware, software, operating systems, networks, storage and user interfaces work together to provide digital functions and services, alongside the role of users, authentication and access control in supporting secure and effective system use. The topic emphasises the interconnected nature of digital systems, the dependencies between components, and how system functionality, performance, reliability, usability and security are influenced by their design and configuration.

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

1.1.1 Digital systems and their components
1.1.2 The role of the operating system in digital systems
1.1.3 Users, authentication and access control

Section	Amplification
1.1.1 Digital systems and their component	Learners should know and understand: • the characteristics of a digital system as a combination of interconnected components that input process, store, transmit and output data to provide digital functions or services • the role of hardware within digital systems, including input, processing, memory, storage output and communication and how the capabilities of hardware influence system functionality and performance • the role of software, including operating systems, application software, utilities and services, in providing instructions and functionality that enable hardware and users to perform required tasks • the role of user interfaces in enabling users to interact with digital systems, including entering data, controlling functions and accessing information • the role of network infrastructure in allowing devices, systems and services to communicate and share data and resources, including network devices, wired and wireless connections and • the role of network communication protocols, in models such as the TCP/IP layer model, in governing how data is formatted, transmitted, received and processed across a network • the role of data storage, including local, networked and cloud-based storage, and how storage requirements can be influenced by capacity, availability, performance, security and access needs • the role of user interfaces as the means through which users interact with digital systems, including graphical, command-based, touch, voice and other interface approaches, and how the choice of interface affects accessibility and usability • how hardware, software, networks, storage, data and interfaces interact as parts of a system rather than functioning independently • how the characteristics and capabilities of individual components can influence the functionality, performance, reliability and usability of the wider system

DRAFT

© WJEC CBAC Ltd 2027.

	• the concept of dependencies within digital systems, where the operation of one component, process or service relies on another, and how changes or failures in one part can affect other parts of the system.
1.1.2 The role of the operating system in digital systems	Learners should know and understand: • the role of an operating system in managing hardware and software resources and providing an environment through which applications and users interact with the system • key operating system functions, including managing processes, memory, files and storage, peripheral devices, network connectivity, users and security • how operating systems coordinate system resources to support multiple applications, services and users • the relationship between operating system configuration and the effective, reliable and secure use of a digital system • why different users and applications may require different levels of access to operating system resources and services.
1.1.3 Users, authentication and access control	Learners should know and understand: • the purpose of user accounts in identifying users and supporting personalised and accountable use of systems • the purpose of authentication in verifying the identity of a user, device or system before access is granted • the purpose of access controls in determining who or what may access systems, services and data and the level of access permitted • how user accounts, authentication and access controls work together to support secure and effective system use • the relationship between user roles, permissions and access to resources, including why access should be appropriate to the tasks a user needs to perform • how inappropriate access can affect the confidentiality, integrity and availability of systems and data • the need to balance secure access with usability so that authorised users can work effectively without unnecessary barriers.
Synoptic links to other Content Areas Knowledge and understanding from this section may contribute to performance in the following areas: • 3.1 Access control, acceptable use and secure system practice • 4.1 Planning and preparing digital systems • 4.2 Digital system configuration and management • 5.2 Analyse, design and communicate digital solutions	

DRAFT

© WJEC CBAC Ltd 2027.

1.2 System configuration and administration

This topic introduces the principles of system configuration and administration that enable digital systems to operate securely, effectively and in line with workplace and user requirements. Learners develop knowledge and understanding of configuration requirements for users, access, connectivity, storage and security, alongside the relationships and dependencies between configuration settings. The topic emphasises the importance of balancing security, usability, accessibility and performance, applying consistent and appropriate configurations, and recognising the risks and consequences of configuration weaknesses, errors and misconfigurations.

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

1.2.1 Configuration requirements
1.2.2 Configuration dependencies and consistency
1.2.3 Configuration for workplace and user requirements
1.2.4 Configuration risks and consequences

Section	Amplification
1.2.1 Configuration requirements	Learners should know and understand: • the purpose of configuration, as setting or adjusting hardware or software parameters so that a system operates correctly and securely for its intended purpose • configuration requirements for user accounts, including the selection of appropriate account types, user roles and account settings to meet system and user requirements • configuration requirements for access permissions, including determining and assigning appropriate levels of access to systems, applications, services and data • configuration requirements relating to connectivity, including access to networks, devices and services and the settings required to support communication • configuration requirements relating to storage, including location, capacity, access and availability requirements (KU1.3) • configuration requirements relating to security settings, including authentication, permissions, updates, network access and protection of systems and data • the characteristics of, and configuration methods for, various types of authentication methods, including: multi-factor authentication, knowledge, possession, biometric, certificate-based, token-based and adaptive • why configuration requirements should be derived from intended purpose, system requirements and user needs rather than settings being selected in isolation.
1.2.2 Configuration dependencies and consistency	Learners should know and understand: • the meaning of a configuration dependency and how one setting, component or service can depend upon another to operate correctly • how dependencies can exist between user accounts, permissions, applications, network services, devices, storage and security settings • how changing configuration settings can produce intended and unintended effects elsewhere within a digital system • why system behaviour should be considered when determining the implications of configuration changes

DRAFT

© WJEC CBAC Ltd 2027.

	• the importance of consistency when configuring systems, including the benefits of using agreed settings, conventions and configuration approaches where users or devices have comparable requirements • how inconsistent configurations can result in differences in functionality, security, usability, support requirements and system behaviour • the benefits and limitations of standardised configurations, including consistency, manageability and security balanced against the need to accommodate legitimate differences in user requirements.
1.2.3 Configuration for workplace and user requirements	Learners should know and understand: • how workplace requirements can influence configuration decisions, including operational practices, security requirements, policies, available infrastructure and technical constraints • how user needs can influence configuration decisions, including requirements relating to functionality, access, usability, accessibility and security • the relationship between configuration choices and system performance, including how allocation and use of system resources can affect effectiveness, usability, speed and reliability • the relationship between configuration choices and usability, including how settings may make a system easier or more difficult for intended users to operate • the relationship between configuration choices and security, including how decisions about access, authentication, authorization, services and system settings alter exposure to risk • how a configuration that meets one requirement can affect another, including potential tensions between security, usability, accessibility and performance • why appropriate configuration depends upon context and there may not be a single configuration that is suitable for all users and organisations.
1.2.4 Configuration risks and consequences	Learners should know and understand: • how misconfigured access permissions can provide excessive, inappropriate or unintended access to systems, services and data • risks associated with weak authentication and authorization settings, including increased likelihood of unauthorised access • risks associated with unpatched software, including exposure to known vulnerabilities and compatibility or reliability problems • risks associated with exposed network services, including unnecessary opportunities for unauthorised or inappropriate access • risks associated with insecure default configurations, including default accounts, credentials, permissions and services that remain unchanged when inappropriate for the intended context • how configuration weaknesses can affect the confidentiality, integrity and availability of systems, services and data • potential consequences of configuration errors for users and organisations, including loss of access, loss or disclosure of information, disruption, poor performance, reduced productivity and security incidents • why configuration risks should be considered in combination, including how separate weaknesses can interact and increase overall system risk.

DRAFT

© WJEC CBAC Ltd 2027.

Synoptic links to other Content Areas
Knowledge and understanding from this section may contribute to performance in the following areas:

- 3.1 Access control, acceptable use and secure system practice
- 3.2 Cyber security threats, vulnerabilities and protective response
- 4.1 Planning and preparing digital systems
- 4.2 Digital system configuration and management
- 5.1 User requirements, analysis and solution planning

DRAFT

© WJEC CBAC Ltd 2027.

1.3 Testing and system readiness

This topic introduces the principles of testing and evaluating digital systems to determine whether they are ready for deployment and use. Learners develop knowledge and understanding of how testing provides evidence that systems meet defined requirements, how test outcomes and performance measures are interpreted, and how functionality, performance, usability and security are assessed against expected standards. The topic emphasises the importance of using evidence-based judgements to evaluate system quality, balance competing priorities and risks, and make informed decisions about system readiness.

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

1.3.1 Requirements and the purpose of testing
1.3.2 Test outcomes and evidence
1.3.3 Performance thresholds and system quality
1.3.4 Performance, usability and security trade-offs
1.3.5 Judging system readiness

Section	Amplification
1.3.1 Requirements and the purpose of testing	Learners should know and understand: • the purpose of testing digital systems to establish whether they behave as expected and meet defined requirements • the relationship between a requirement, the conditions or capabilities that must be satisfied, and a test, which provides evidence about whether they have been satisfied • different characteristics of a system that may form the basis of requirements and tests, including functionality, performance, reliability, usability, accessibility and security-related behaviour • the importance of defining expected outcomes so that actual system behaviour can be compared with what should occur • how requirements need to be sufficiently clear and measurable to enable meaningful judgements about whether they have been met • how test coverage influences confidence in system readiness, including the need for testing to reflect significant system requirements and realistic patterns of use • how dependencies between system components can influence the scope and sequence of testing.

DRAFT

© WJEC CBAC Ltd 2027.

1.3.2 Test outcomes and evidence	Learners should know and understand: • the relationship between test conditions, expected outcomes, observed outcomes and conclusions about whether requirements have been met • how test outcomes can provide evidence of compliance with individual requirements but do not automatically demonstrate that a complete system is ready for use • how repeated or related test outcomes can reveal patterns, including intermittent, recurring or context-dependent issues • why unexpected outcomes require interpretation to determine their significance rather than being treated automatically as equivalent in severity • how system information such as logs, alerts and performance indicators can provide supporting evidence when interpreting test outcomes • factors that can affect the reliability of test evidence, including unsuitable test conditions, incomplete coverage, inconsistent procedures and differences between test and intended operating environments • why test findings should be sufficiently clear, accurate and consistent to allow evidence to support subsequent decisions about system readiness.
1.3.3 Performance thresholds and system quality	Learners should know and understand: • the purpose of performance thresholds as predefined measures used to evaluate system performance • examples of characteristics for which thresholds may be defined, such as response time, resource utilisation, capacity, availability, reliability and error rates • the distinction between a system functioning and a system performing at a level that is acceptable for its intended use • why appropriate thresholds depend on system purpose, workplace context, user requirements and the consequences of inadequate performance • how patterns across multiple performance indicators can provide a more meaningful view of system behaviour than a single measure considered in isolation • how performance below an agreed threshold can affect user experience, productivity and reliability even when core system functions remain available.
1.3.4 Performance, usability and security trade-offs	Learners should know and understand: • the meaning of a trade-off, where improving or prioritising one characteristic of a system may adversely affect another • potential relationships between performance and security, for example where additional security controls require processing or introduce additional stages into user interaction • potential relationships between security and usability, for example where stronger access controls increase protection but also increase the effort required from authorised users • potential relationships between performance and usability, including how system responsiveness and reliability can influence the effectiveness of interaction

DRAFT

© WJEC CBAC Ltd 2027.

	• why a trade-off does not mean that one characteristic should automatically take priority, and why decisions should reflect the defined requirements, context and level of risk • how requirements and thresholds can be used to distinguish acceptable compromises from outcomes that make a system unsuitable for its intended use.
1.3.5 Judging system readiness	Learners should know and understand: • the concept of system readiness and how evidence from testing informs decisions about deployment or continued use • how test results should be considered collectively against defined requirements rather than treating each outcome independently • how the severity, likelihood and impact of unresolved issues can influence a readiness decision • why a system may meet some requirements and fail others, and how the significance of unmet requirements depends on their importance to intended use • possible conclusions from assurance activity, including that a system is ready for use, ready subject to acceptable limitations, requires further adjustment or requires further investigation and testing • why continued use can also require assurance, particularly where systems, requirements, configurations or operating environments change • how readiness decisions should balance evidence about functionality, performance, usability and security rather than assuming readiness because a system performs its principal function • the role of reasoned judgement where evidence is incomplete or outcomes conflict, including recognising uncertainty rather than overstating confidence in readiness.

Synoptic links to other Content areas
Knowledge and understanding from this section may contribute to performance in the following areas:

- 4.1 Planning and preparing digital systems
- 4.4 Testing, validation and quality assurance
- 5.1 User requirements, analysis and solution planning
- 5.4 User-centred, secure and responsible digital solution design

DRAFT

© WJEC CBAC Ltd 2027.

1.4 Fault diagnosis and technical support

This topic introduces the principles of fault diagnosis and technical support within digital systems. Learners develop knowledge and understanding of the causes of hardware, software, network and user-related faults, and how system behaviour can be interpreted to identify and investigate issues. The topic emphasises the use of structured, evidence-based approaches to diagnosing and resolving faults, while considering the operational, security, legal and ethical responsibilities involved in managing technical issues and maintaining effective system performance.

In this topic learners will gain knowledge and understanding in the following areas:
1.4.1 Nature and causes of technical faults
1.4.2 Interpreting system behaviour
1.4.3 Structured fault diagnosis and resolution
1.4.4 Consequences and responsible fault management

Section	Amplification
1.4.1 Nature and causes of technical faults	Learners should know and understand: • what constitutes a technical fault, including failures, errors or unexpected behaviours that prevent a system or component from meeting expected outcomes • hardware-related faults, including component failure, physical damage, connection problems, capacity or resource limitations and incompatible components • software-related faults, including incorrect configuration, corrupted or incompatible software, update-related issues, application failures and resource conflicts • network-related faults, including loss or degradation of connectivity, inappropriate network configuration and failure of network components or services • user-related factors that can contribute to reported faults, including inappropriate settings, incorrect operation, access or authentication problems and misunderstanding of expected system behaviour • how apparently similar issues can have different underlying causes and how a single underlying fault can produce multiple issues • the distinction between an issue, which is an observable indication of a problem, and a cause, which explains why it occurs • how dependencies within digital systems can cause faults originating in one component or service to affect apparently unrelated functions.
1.4.2 Interpreting system behaviour	Learners should know and understand: • how comparison between expected and observed behaviour supports identification of faults • how the circumstances in which a fault occurs, including timing, affected users, affected functions and preceding changes, can provide evidence about possible causes • how patterns such as repeated errors, intermittent failures, reduced performance or loss of connectivity can help distinguish between possible fault types • why correlation between a change and a fault does not on its own establish causation and additional evidence may be required • how the scope of a problem, for example whether it affects one user, one device, a group of users or an entire service, can help narrow potential causes

DRAFT

© WJEC CBAC Ltd 2027.

	• why accurate understanding of normal system behaviour provides a useful basis for recognising deviations and diagnosing faults.
1.4.3 Structured fault diagnosis and resolution	Learners should know and understand: • the purpose of a structured approach to fault diagnosis in reducing assumptions and supporting consistent, evidence-based decision making • stages in a logical diagnostic process, including gathering information, establishing expected behaviour, identifying anomalies/issues or indicators of concern, gathering and interpreting evidence, narrowing down potential causes, and determining an appropriate response • the value of using available evidence to identify and evaluate plausible causes before determining an appropriate response or making changes to a system the role of diagnostic tools, including tools that provide information about hardware, software, network connectivity, resource use and system status • the role of system and software information, including system logs, error messages, alerts, status information and performance indicators, in identifying and distinguishing possible causes • how testing a hypothesis through controlled changes or checks can support systematic identification of the source of a fault • why changes made during diagnosis can themselves affect system behaviour and should therefore be considered systematically • the purpose of escalation when an issue cannot or should not be resolved at the current level of responsibility • factors influencing escalation decisions, including complexity, permissions, risk, potential impact, urgency and organisational procedure • the importance of restoring system functionality while avoiding unnecessary changes or additional disruption.
1.4.4 Consequences and responsible fault management	Learners should know and understand: • potential consequences of inaccurate diagnosis, including unnecessary changes, additional faults, security risks, loss of data, avoidable disruption and delayed restoration • potential consequences of delayed action, including prolonged service disruption, reduced productivity, increased security or data risks and impacts on users • the importance of protecting personal and sensitive information while gathering diagnostic information and resolving faults • requirements to maintain confidentiality and privacy, including avoiding unnecessary access to or disclosure of user data during diagnosis • the importance of preserving system integrity, including avoiding changes that introduce new vulnerabilities or compromise system reliability • the importance of preserving availability and security, including considering disruption to users and services before making changes • how legal and ethical responsibilities constrain the information that can be accessed, changed, recorded or shared during technical support activity • the need to consider the wider effects of diagnostic and resolution actions on users, services and organisations

DRAFT

© WJEC CBAC Ltd 2027.

	• why technically effective action may still be inappropriate if it creates unacceptable privacy, security, ethical or operational consequences.

Synoptic links to other Content Areas
Knowledge and understanding from this section may contribute to performance in the following areas:

- 3.1 Access control, acceptable use and secure system practice
- 3.2 Cyber security threats, vulnerabilities and protective response
- 3.3 Monitoring and interpreting system information for security indicators
- 4.5 System monitoring, fault diagnosis and resolution

DRAFT

© WJEC CBAC Ltd 2027.

1.5 Communication and user support

This topic introduces the principles of communication and user support within technical environments. Learners develop knowledge and understanding of how effective communication supports the identification, investigation and resolution of technical issues, including the use of appropriate questioning, information gathering and escalation processes. The topic emphasises the importance of adapting communication to meet the needs of different users, providing clear and accessible support, and communicating professionally, ethically and responsibly while maintaining accuracy, confidentiality and user confidence.

In this topic learners will gain knowledge and understanding in the following areas:
1.5.1 Communication in technical support
1.5.2 Adapting communication for users
1.5.3 Professional, ethical and responsible communication

Section	Amplification
1.5.1 Communication in technical support	Learners should know and understand: • the role of communication in establishing the nature, context, impact and history of a technical issue • how information provided by users can contribute evidence about issues, such as unusual system behaviour, unexpected errors, or performance problems, alongside expected behaviour and the circumstances surrounding an incident • how questioning can be used to clarify reported issues, verify observed behaviour, establish relevant facts, and distinguish evidence-based observations from assumptions or opinions • why technical information from users, systems and other sources may need to be interpreted and combined to create an accurate understanding of an issue • the importance of communicating relevant information accurately when an issue is transferred or escalated to others • how effective communication supports continuity and efficiency of technical support by reducing ambiguity, repetition and misunderstanding • the distinction between communication-based support, such as explanation, guidance or clarification, and technical troubleshooting, which involves investigation of system behaviour and possible technical causes.
1.5.2 Adapting communication for users	Learners should know and understand: • how communication choices can affect clarity, efficiency and user experience during technical support • why language, terminology, level of detail and structure should be appropriate to the knowledge and needs of the intended audience • how technical terminology can support precision when communicating with knowledgeable audiences but may reduce understanding when used inappropriately with non-technical users • how communication formats can affect users' ability to understand and respond to support information • how accessibility and other diverse user needs may require adaptations to language, format, pace, structure or communication format

DRAFT

© WJEC CBAC Ltd 2027.

	• the importance of confirming shared understanding rather than assuming that information has been understood because it has been communicated • how clear explanations of actions, expectations and next steps can support effective service delivery and user confidence in the support process.
1.5.3 Professional, ethical and responsible communication	Learners should know and understand: • the importance of accuracy and consistency when recording and communicating technical information • the need to distinguish facts and evidence from assumptions, interpretations and recommendations when communicating technical issues • how appropriate technical and non-technical language supports accurate communication with different audiences • responsibilities relating to confidentiality and privacy when technical information includes personal, sensitive or security-related information • why information should only be shared with appropriate people and to the extent necessary for the support purpose • principles for responding professionally to user queries and expectations, including clarity about what can be resolved, what requires further investigation and what may need to be escalated • how unclear, inaccurate or inappropriate communication can contribute to incorrect diagnosis, ineffective support, loss of user confidence and privacy or security risks.

Synoptic links to other Content Areas
Knowledge and understanding from this section may contribute to performance in the following areas:

- 2.1 Understanding the purpose and structure of data
- 2.2 Preparing, validating and documenting data
- 2.3 Analytical techniques and drawing conclusions
- 2.6 Presenting and communicating
- 4.5 System monitoring, fault diagnosis and resolution
- 5.4 User-centred, secure and responsible digital solution design
- 5.5 Analyse, design and communicate digital solutions

DRAFT

© WJEC CBAC Ltd 2027.

1.6 Collaboration and requirements analysis

This topic introduces the principles of collaboration and requirements analysis in the development of digital solutions. Learners develop knowledge and understanding of how different stakeholders contribute to decision making, how user needs are identified and interpreted, and how these needs are translated into clear and effective solution requirements. The topic emphasises the importance of collaborative working, inclusive and evidence-based decision making, and the consideration of technical, organisational and resource constraints when designing digital solutions that meet user and organisational needs.

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

1.6.1 Collaboration in digital work
1.6.2 Identifying and interpreting user needs
1.6.3 Translating needs into digital solution requirements
1.6.4 Constraints and inclusive decision making

Section	Amplification
1.6.1 Collaboration in digital work	Learners should know and understand: • the role of collaboration in developing digital solutions where effective outcomes require contributions from people with different responsibilities, knowledge and expertise • how different roles and perspectives can contribute technical, organisational, user, accessibility, security and other relevant considerations to decision making • how combining different forms of expertise can identify issues, requirements and opportunities that may not be apparent from a single perspective • how differences in priorities and perspectives can influence decisions about a proposed digital solution • the value of structured collaborative approaches in establishing responsibilities, sharing information, recording decisions and maintaining a common understanding including version control, tracking changes, real time co-editing • how clear responsibilities and agreed methods for collaboration support consistency, accountability and effective decision making • risks associated with ineffective collaboration, including incomplete requirements, conflicting assumptions, inconsistent decisions, duplication and gaps in responsibility.

DRAFT

© WJEC CBAC Ltd 2027.

1.6.2 Identifying and interpreting user needs	Learners should know and understand: • the distinction between a user need, which identifies a problem or objective, and a user requirement, which defines the functionality that needs to be addressed • why stated requests do not necessarily represent the complete underlying need and may require interpretation and clarification • how information from users and other relevant stakeholders contributes to identifying the purpose and expected outcomes of a digital solution • how diverse users may have different requirements arising from their tasks, circumstances and accessibility needs • why assumptions about users can lead to requirements that are incomplete, inappropriate or exclusionary • the importance of shared understanding of user needs before significant design decisions are made, including the principles of secure by design.
1.6.3 Translating needs into digital solution requirements	Learners should know and understand: • how identified user needs can be translated into requirements that inform the design of digital solutions • how requirements clarify the functionality, user interaction and outcomes expected from a proposed solution • how requirements can be refined as understanding of the problem and users improves • the role of feedback in checking whether interpretations and proposed designs reflect actual user needs • the role of iteration in progressively refining requirements and designs in response to feedback and emerging understanding • how shared understanding between users, collaborators and those developing a solution reduces ambiguity and conflicting interpretation • why changes to requirements can have consequences for other aspects of a design and should be considered in relation to dependencies and constraints.
1.6.4 Constraints and inclusive decision making	Learners should know and understand: • technical constraints that can affect digital solution decisions, including available technologies, compatibility, infrastructure, integration requirements and technical capabilities • organisational constraints that can influence decisions, including policies, procedures, existing systems, working practices and governance requirements • resource constraints, including time, available expertise, equipment, infrastructure and financial resources • how constraints can affect the feasibility, scope, complexity and priorities of proposed digital solutions • how multiple constraints may interact and require trade-offs rather than being considered independently • why constraints should be identified and understood rather than automatically treated as fixed barriers, including distinguishing genuine constraints from assumptions • the importance of inclusive collaboration, ensuring that relevant perspectives and diverse user needs inform decision making • principles of responsible collaborative decision making, including using evidence, recognising competing requirements, considering impacts and documenting reasons for significant decisions.

DRAFT

© WJEC CBAC Ltd 2027.

Synoptic links to other Content Areas
Knowledge and understanding from this section may contribute to performance in the following areas:

- 4.1 Planning and preparing digital systems
- 4.3 Usability, accessibility and inclusive practice
- 5.1 User requirements, analysis and solution planning
- 5.5 Analyse, design and communicate digital solutions

DRAFT

© WJEC CBAC Ltd 2027.

1.7 Digital systems design and development

This topic introduces the principles of designing and developing digital solutions to meet defined user and organisational needs. Learners develop knowledge and understanding of structured problem solving, computational thinking, algorithms and solution logic, and how these are applied to analyse problems and create effective digital solutions. The topic emphasises the use of logical, structured approaches to solution design, development, testing and refinement, ensuring that digital solutions are reliable, maintainable and fit for purpose.

In this topic learners will gain knowledge and understanding in the following areas:
1.7.1 Structured problem solving
1.7.2 Algorithms, solution logic and control structures
1.7.3 Designing structured digital solutions
1.7.4 Developing, testing and refining solutions

Section	Amplification
1.7.1 Structured problem solving	Learners should know and understand: • the purpose of structured problem solving in developing digital solutions that address defined needs rather than immediately selecting a technology or implementation approach • how a problem can be analysed in terms of its purpose, required outcomes, inputs, processes, outputs, requirements and constraints • computational thinking involves decomposition, pattern recognition, abstraction and algorithmic design to solve problems and create solutions that can be followed by humans or computers • the role of decomposition in breaking a complex problem or system into smaller, more manageable parts, including understanding the dependencies and interfaces between components that must be considered when recombining them into an overall solution • the role of pattern recognition in identifying similarities, trends, repeated processes, or common features within problems, allowing existing knowledge and solutions to be reused • the role of abstraction in identifying and representing information and characteristics relevant to the problem while excluding unnecessary detail and how the appropriate level of abstraction depends on the purpose and stage of problem solving • the role of algorithms in developing clear, logical, and ordered sets of instructions to solve problems and produce desired outcomes and that they can be designed, tested, refined, and implemented to achieve efficient and accurate solutions • how computational thinking can reduce complexity, support planning, and make solutions easier to understand, develop, and test • limitations of inappropriate application of computational thinking techniques, including omitting important information, dividing a problem at unsuitable points, identifying incorrect or misleading patterns or developing algorithms that are inefficient, incomplete, or fail to solve the problem effectively.

DRAFT

© WJEC CBAC Ltd 2027.

1.7.2 Algorithms, solution logic and control structures	Learners should know and understand: • the purpose of an algorithm as a defined sequence of instructions used to process inputs, produce outputs or solve a problem • how algorithms represent solution logic independently of the specific technology that may ultimately implement the solution • the importance of clarity, precision and logical ordering when defining algorithmic processes • how variables or data items can represent values that are stored, accessed or changed while a solution operates • how structured representations of algorithms support communication, checking and refinement before or during implementation • sequencing as arranging instructions or processes in the required logical order • selection as using defined conditions to determine which path through a process should be followed • how single and multiple conditions can influence selection between alternative outcomes • iteration as repeating instructions or processes according to defined conditions or for a defined number of repetitions • the distinction between repetition controlled by a condition and repetition controlled by a predetermined number or set of items • how sequencing, selection and iteration can be combined to represent more complex solution behaviour • how incorrect conditions or controls can lead to unintended paths, unnecessary repetition, missed processing or failure to terminate correctly • why logic should account for alternative, boundary and unexpected inputs rather than considering only the most straightforward route through a solution.
1.7.3 Designing structured digital solutions	Learners should know and understand: • how problem analysis, abstraction, decomposition and programming logic contribute collectively to digital solution design • how a proposed solution can be structured into components or processes with clearly defined purposes and relationships • how modular approaches can support understandability, testing, reuse, maintenance and refinement by separating parts of a solution according to their responsibilities • how design choices affect the reliability and maintainability of a digital solution • the value of avoiding unnecessary complexity where a simpler logical structure can meet the same requirements • how requirements and constraints influence which solution structures and logical approaches are appropriate • how solution logic should reflect intended user interactions and expected system behaviour • how documenting logic and design decisions supports understanding and later development or modification of a solution.

DRAFT

© WJEC CBAC Ltd 2027.

1.7.4 Developing, testing and refining solutions	Learners should know and understand: • the relationship between design and development, including how a structured design provides a basis for creating a digital solution • how implementation can reveal assumptions, dependencies or weaknesses not identified during initial design • why testing should be related to the intended requirements and expected behaviour of the solution • the role of test inputs and expected outputs in establishing whether solution logic behaves as intended, including how the solution should respond to normal, boundary, invalid and unexpected inputs • the distinction between identifying that a solution produces an incorrect result and establishing the logical cause of that result • how tracing logic and examining intermediate states can support identification of errors in structured solutions • the role of refinement in changing a design or implementation in response to test outcomes, identified weaknesses, feedback or improved understanding, judged against requirements so that changes improve fitness for purpose • iterative development as repeated cycles of designing, developing, testing, evaluating and refining, rather than a single linear process • how changes made during refinement can introduce new errors or unintended effects, requiring further testing.
Synoptic links to other Content Areas Knowledge and understanding from this section may contribute to performance in the following areas: • 5.2 Analyse, design and communicate digital solutions	

DRAFT

© WJEC CBAC Ltd 2027.

1.8 AI, Ethics and responsible digital practice

This topic introduces the principles of artificial intelligence (AI) and responsible digital practice in modern digital environments. Learners develop knowledge and understanding of AI concepts, including machine learning, data, algorithms and models, alongside the capabilities and limitations of AI-enabled systems and the role of human oversight in decision making. The topic emphasises the effective and responsible use of AI, including the creation and evaluation of prompts and outputs, and the ethical, legal, social and environmental considerations that underpin responsible digital practice.

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

1.8.1 Artificial intelligence fundamentals
1.8.2 Data, algorithms, models and machine learning
1.8.3 AI capabilities, limitations and decision making
1.8.4 Prompts, structured inputs and generated outputs
1.8.5 Ethical, legal, social and sustainable digital practice

Section	Amplification

1.8.1 Artificial intelligence fundamentals	Learners should know and understand:
	• artificial intelligence (AI) as a field concerned with digital systems capable of performing tasks involving capabilities commonly associated with intelligent behaviour
	• how AI functions at a basic level, including how AI systems use computational methods to process inputs, identify or apply patterns and generate outputs
	• the distinction between traditional rule-based automated systems, where behaviour is determined through predefined rules, and AI approaches in which model behaviour can be developed by learning patterns from data
	• the relationship and distinctions between:
	  • artificial intelligence, as the broad field of systems that perform tasks normally requiring human intelligence, using approaches such as programmed rules or learning from data
	  • machine learning, a subset of AI in which models learn patterns from data to make predictions or decisions without being explicitly programmed for each case
	  • deep learning, a subset of machine learning that uses multi-layered neural networks and is suited to complex tasks such as image and speech recognition
	  • generative AI, typically built using deep learning, which produces new content in response to inputs or prompts
	• types of AI, including:
	  • by capability: AI designed for defined or narrow purposes, and the concept of more general AI capability
	  • by function: systems that classify, predict, recommend, recognise patterns, support decisions or generate content
	  • by field of application: natural language processing, computer vision, speech recognition, data analysis, recommendation, automation and system monitoring
	  • how AI-enabled systems use data, algorithms or models to generate outputs such as predictions, classifications, insights or recommendations, and how the quality and quantity of training data affect the reliability of those outputs.

DRAFT

© WJEC CBAC Ltd 2027.

1.8.2 Data, algorithms, models and machine learning	Learners should know and understand:
	• the relationship between data, algorithms and models, including:
	  • data as the facts, measurements or examples from which patterns can be identified
	  • algorithms as the processes used to analyse data and build a model
	  • models as the learned or constructed representations used to generate outputs from new inputs
	• examples of AI model types and purposes, including:
	  • classification: assigning inputs to categories
	  • prediction and regression: estimating values or future outcomes
	  • clustering: grouping similar data without predefined categories
	  • recommendation: suggesting items based on patterns in preferences or behaviour
	  • recognition: identifying objects, speech, faces or text
	  • generative models: producing new content
	• how machine-learning models learn from data at a high level, including:
	  • the role of training data as the foundation from which a model identifies patterns and relationships
	  • the distinction between:
	  • training data, used to develop or fit a model
	  • validation data, used to tune and adjust the model during development
	  • test data, used to evaluate performance on data the model has not seen
	  • supervised learning at a high level, where a model learns from training examples associated with known or labelled outcomes
	  • unsupervised learning at a high level, where techniques identify structures or patterns within data without predetermined outcome labels
	• why data quality matters when developing and using AI models, including the importance of:
	  • accuracy
	  • completeness
	  • relevance
	  • currency
	  • representativeness
	• how poor-quality, inaccurate, incomplete, outdated or unrepresentative data can affect the reliability and usefulness of AI outputs
	• why performance on training data does not in itself demonstrate that a model will perform reliably with new or different data.

DRAFT

© WJEC CBAC Ltd 2027.

1.8.3
AI capabilities, limitations and decision making
	Learners should know and understand:
	• capabilities of AI, including:
	  • processing large quantities of data
	  • identifying patterns
	  • automating or accelerating defined tasks
	  • generating content
	  • supporting prediction, classification and decision making
	• potential benefits of using AI, including:
	  • increased efficiency
	  • scalable processing
	  • identification of patterns within large quantities of data
	  • support for complex analysis
	  • automation of repetitive activities
	  • augmentation of human decision making
	• limitations of AI-enabled systems, including dependence on their data and design, incomplete understanding of context, potential for inaccurate outputs and the inability to guarantee that outputs are factually accurate
	• why apparently convincing or plausible AI-generated outputs may be inaccurate, inappropriate or affected by bias, and the implications this can have where outputs inform decisions
	• how bias can arise in AI-enabled decision making, including through the data used, assumptions made during system development, model design, system objectives and the context in which a system is deployed
	• how bias in AI-enabled systems can result in different or unfair outcomes for users or groups, and why computational processing does not in itself guarantee impartial outcomes
	• the risks of relying on AI-generated recommendations or automated decisions without appropriate interpretation and validation
	• the need for human oversight when AI-enabled systems contribute to decision making, including reviewing outputs, applying contextual and professional judgement, identifying potential errors or bias and retaining appropriate human accountability
	• how the level of human oversight required can be influenced by the purpose of an AI-enabled system, the potential consequences of a decision, the people affected and the reliability of the system
	• circumstances in which the limitations, uncertainty or potential consequences associated with an AI-enabled system may mean that it should not be used for a particular decision or that additional controls and human review are required.

1.8.4 Prompts, structured inputs and generated outputs	Learners should know and understand: • the role of a prompt or structured input in providing an AI-enabled system with information or instructions that influence the output generated • characteristics of prompts that can affect outputs, including clarity of purpose, relevant context, constraints, specified format and level of detail • how ambiguous, incomplete, conflicting or overly broad inputs can reduce the relevance or usefulness of generated outputs • how providing relevant context and clearly defining the required outcome can improve alignment between an output and its intended

© WJEC CBAC Ltd 2027.

	purpose • how different prompts or variations in input may produce different outputs from the same AI-enabled system • why effective prompt design cannot guarantee that an AI-generated output will be factually accurate, unbiased or suitable • the role of iterative prompting in refining generated outputs, including using evaluation of an initial output to inform subsequent inputs • why generated outputs should be reviewed in relation to their purpose, accuracy, relevance, completeness, limitations and possible bias • risks associated with including personal, sensitive, confidential or otherwise inappropriate information within prompts or other inputs to AI-enabled systems • why users should understand that prompts can shape outputs and therefore influence subsequent interpretation or decisions.

1.8.5 Ethical, legal, social and sustainable digital practice	Learners should know and understand:
	• characteristics of responsible digital practices
	• ethical considerations relating to digital practice, including fairness, transparency, accountability, privacy, inclusion and avoidance of harm
	• how the use of automated and AI-enabled systems can have different impacts on users and groups, including where systems influence access, opportunities, recommendations or decisions
	• why transparency about the use and limitations of automated and AI-generated outputs supports informed interpretation and responsible use
	• the importance of accountability, including recognising that responsibility for decisions cannot automatically be transferred to an automated or AI-enabled system
	• legal considerations, including laws applicable to digital practice including:
	  • UK General Data Protection Regulation **(**GDPR) and the Data Protection Act 2018
	  • Copyright, Designs and Patents Act 1988
	  • Computer Misuse Act 1990
	  • Equality Act 2010
	  • Freedom of Information Act 2000
	  • Privacy and Electronic Communications Regulations (PECR) 2003 and how these influence the handling of information, security of digital systems, accessibility of digital products and services, and compliance with organisational and legal requirements
	• the purpose of intellectual property rights in protecting creations and the relevance of such rights to digital materials
	• considerations relating to ownership and attribution when using, adapting or creating digital material, including material produced with the support of automated and AI-enabled systems
	• why the source, permitted use and ownership status of material should be considered before it is reproduced, adapted or incorporated into a digital output
	• ethical and intellectual-property questions that can arise where AI systems are trained on, transform or generate material derived from existing content
	• principles of responsible use of automated and AI-enabled systems, including selecting appropriate uses, understanding limitations,

© WJEC CBAC Ltd 2027.

	reviewing outputs, protecting information, being transparent about use where relevant and maintaining human responsibility • sustainability considerations associated with digital practice, including energy and resource use, data storage and processing, device manufacture and lifecycle and the environmental implications of operating digital and AI-enabled systems at scale • how choices about hardware, storage, processing, system use and device lifecycle can influence resource and energy requirements • why responsible digital practice requires ethical, legal, social, environmental and operational considerations to be balanced rather than considered independently.

Synoptic links to other Content Areas

Knowledge and understanding from this section may contribute to performance in the following areas:

- 2.1 Understanding the purpose and structure of data
- 2.4 Automated and AI-enabled analysis
- 2.5 Data ethics, privacy, inclusion and sustainability
- 3.3 Monitoring and interpreting system information for security indicators
- 4.2 Digital system configuration and management
- 4.4 Testing, validation and quality assurance
- 5.3 Prototyping and development approaches

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 2 Data Analysis and Insights

GLH	80
Overview of content area	This content area develops the knowledge, understanding and skills required to collect, manage, analyse and interpret data to support decision-making. Learners explore how data is sourced, structured and processed, and how analytical techniques can be used to identify patterns, trends and relationships within datasets. They develop an understanding of how data is used to generate insights, solve problems and inform decisions across a range of digital and organisational contexts. The content area provides learners with the foundations of data literacy, enabling them to evaluate the quality, reliability and relevance of data, apply appropriate analytical methods, and communicate findings effectively to different audiences. Learners also develop an understanding of the ethical, legal and security considerations associated with collecting, storing, analysing and sharing data. The knowledge and understanding developed through this content area builds upon the core knowledge and understanding established in Content Area 1. Together, these content areas provide the conceptual foundation that underpins achievement across the qualification. Where concepts are reflected across both content areas, the core knowledge and understanding from Content Area 1 defines what learners are expected to know and understand, while the knowledge and understanding in this content area provides opportunities to apply that knowledge in context. Through engagement with the activities, scenarios and tasks contained within the work-related purposes, learners are expected to apply, demonstrate and extend their knowledge and understanding in authentic vocational contexts. These experiences provide opportunities for learners to further develop and deepen their core knowledge and understanding while using data to generate insights, inform decision-making and support the development of effective digital solutions.
Topics	2.1 Understanding the purpose and structure of data 2.2 Preparing, validating and documenting data 2.3 Analytical techniques and drawing conclusions 2.4 Automated and AI-enabled analysis 2.5 Data ethics, privacy, inclusion and sustainability 2.6 Presenting and communicating
Summary of assessment	Non-exam assessment Assessment 3: Data Analysis and Insights • 20 hours • Set by WJEC, centre marked, moderated by WJEC • 80 marks

DRAFT

© WJEC CBAC Ltd 2027.

Resources required for assessment	Candidates will require access to suitable digital devices, software and datasets that enable them to prepare, analyse and present data. Where required by the assessment, candidates must also have access to AI-enabled analytical tools. Centres are responsible for ensuring that all software, tools and resources required to complete the assessment are available to candidates.

Content

2.1 Understanding the purpose and structure of data

This topic introduces the principles of working with data to support informed decision making in digital and workplace contexts. Learners develop knowledge and understanding of how data is prepared, analysed, interpreted and presented to generate meaningful insights and conclusions, alongside the importance of considering audience and purpose. The topic emphasises the structure, format and quality of data, and how these factors influence the reliability, suitability and effectiveness of analysis and the decisions that result from it.

In this topic learners will gain knowledge, understanding and skills in the following areas:
2.1.1 Data driven decision making
2.1.2 Data structure, format, and definitions across sources
2.1.3 The importance of data quality

Section	Amplification

2.1.1 Data driven decision making	Learners should know and understand:
	• that how a dataset is prepared, analysed, interpreted and presented will vary depending on factors such as:
	  ◦ the intended audience
	  ◦ the purpose of the analysis
	  ◦ the decision it is intended to support
	• the difference between data, analysis, insight and conclusion, including:
	  ◦ data: raw recorded facts and figures (for example, the number of products sold in a day)
	  ◦ analysis: examining the data to find a pattern (for example, spotting a downward trend in sales)
	  ◦ insight: identifying patterns, trends or relationships in data and explaining their significance in a workplace context. (for example, why sales are falling in a particular region)
	  ◦ conclusion: summarising the key findings and recommending an action based on insights (for example, proposing that stock levels be reduced in that region)
	• the relationship between analytical findings and presentation choices and user interpretation of information.
	
	Learners should be able to use a variety of datasets from different sources to:
	• prepare datasets, from a range of sources, for analysis
	• identify the purpose of data analysis and explain how the findings can support decision making
	• examine data from different sources to determine its suitability for analysis, including whether it is relevant, reliable and sufficient to achieve the intended purpose

© WJEC CBAC Ltd 2027.

	• examine data from different sources to determine its suitability for analysis, including whether it is relevant, reliable and sufficient to achieve the intended purpose
	• prepare data for analysis by validating it, checking formats and confirming that it is complete and accurate
	• analyse prepared datasets to identify patterns, relationships and trends
	• examine analytical outputs in relation to the defined decision-making purpose
	• interpret analysed datasets to produce results in a workplace context
	• interpret analytical results and consider potential sources of bias and limitation in the data
	• draw reasoned conclusions from analysed data
	• present results of data analysis in a suitable format that:
	  • considers the needs of the audience including inclusivity and accessibility for diverse users
	  • includes graphical and tabular visualisations to present insights clearly and accurately
	  • is suitable for the defined purpose and workplace context
	• ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations
	• communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences
	• document analytical decisions, assumptions and outputs clearly review presented outputs to improve clarity, accessibility and relevance.

2.1.2 Data structure, format, and definitions across sources	Learners should know and understand: • the difference between how data is structured and formatted • that data can be defined differently across the same or different systems • how levels of detail affect interpretation • how differences in structure, format and definition between sources affect comparability and compatibility between systems • that a dataset's suitability depends on its intended use. Learners should be able to examine and compare data from different sources, including their structure, format, definitions and level of detail, to determine suitability for a stated analytical purpose.

2.1.3 The importance of data quality	Learners should know and understand:
	• the impact that data quality can have on a data set and analysis, including:
	  • missing data
	  • duplicate records
	  • conflicting values
	  • inconsistent data formats
	  • falsified data
	that unresolved data quality issues can impact conclusions.

© WJEC CBAC Ltd 2027.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.5.1 Communication in technical support
- 1.5.2 Adapting communication for users
- 1.8.1 Artificial intelligence fundamentals
- 1.8.3 AI capabilities, limitations and decision making
- 1.8.5 Ethical, legal, social and sustainable digital practice

DRAFT

© WJEC CBAC Ltd 2027.

2.2 Preparing, validating and documenting data

This topic introduces the principles of preparing, validating and documenting data to support accurate and reliable analysis. Learners develop knowledge and understanding of data validation techniques, the identification and resolution of data quality issues, and the importance of documenting decisions, assumptions and corrections made during data preparation. The topic emphasises the effective use and combination of datasets from different sources, the role of metadata and field definitions in supporting interpretation, and the importance of transparency, consistency and accountability throughout the analytical process.

In this topic learners will gain knowledge, understanding and skills in the following areas:
2.2.1 Data validation and preparation
2.2.2 Combining datasets

Section	Amplification
2.2.1 Data validation and preparation	Learners should know and understand: • the methods used to validate and prepare data prior to analysis, including: • data type and format checking • verifying of value ranges • resolving inconsistencies • confirming completeness. Learners should be able to: • prepare data for analysis through validation, checking formats and confirming completeness • resolve inconsistencies such as duplicate records, conflicting values, or misaligned definitions, deciding how each should be handled (for example corrected, merged, removed, or flagged) • document the assumptions or corrections made during preparation, so the process is traceable and can be checked or replicated by someone else.

2.2.2 Combining datasets	Learners should know and understand:
	• the role of metadata and field definitions in data analysis
	• the purpose of using documentation to support data analysis, such as:
	  • data sources
	  • metadata and field definitions used
	  • corrections and assumptions made
	  • validation carried out
	• how metadata, field definitions and documentation support accountability, transparency and correct interpretation of analysed outputs
	• the risks associated with analysing and combining datasets from different data sources, such as:
	  • inaccurate assumptions
	  • missed relationships and insights
	  • inconsistent definitions
	  • mismatched level of detail

DRAFT

© WJEC CBAC Ltd 2027.

	Learners should be able to use and combine a variety of datasets to work towards a stated analytical purpose, including: • analyse prepared datasets to identify patterns, relationships and trends • preparing data for analysis through validation, checking formats and confirming completeness examining data from different sources, using available metadata and field definitions, to determine its suitability for a stated analytical purpose.
Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.5.1 Communication in technical support • 1.5.2 Adapting communication for users	

DRAFT

© WJEC CBAC Ltd 2027.

2.3 Analytical techniques and drawing conclusions

This topic introduces the techniques used to analyse data and generate meaningful conclusions to support decision making. Learners develop knowledge and understanding of a range of analytical methods, how analytical outputs such as summaries, comparisons, trends and indicators are produced and interpreted, and the role of professional judgement in drawing conclusions from data. The topic emphasises the importance of selecting appropriate analytical techniques, recognising limitations and sources of uncertainty, and communicating clear, evidence-based findings that are relevant to the intended purpose and audience.

In this topic learners will gain knowledge, understanding and skills in the following areas:
2.3.1 Analytical techniques
2.3.2 Analytical outputs
2.3.3 Interpretation and professional judgement in generating conclusions

Section	Amplification

2.3.1 Analytical techniques	Learners should know and understand:
	• the range of analytical tools and techniques that can be used in data analysis, including: (WRP1.5)
	  • sorting
	  • filtering
	  • grouping records
	  • calculating totals, averages and percentages
	  • rates of change
	  • comparing categories
	  • ranking results
	• how comparing categories and ranking results helps identify which items, groups or periods stand out relative to others
	• what trends, patterns and anomalies look like in data
	• that different techniques suit different data types and analytical purposes (for example ranking suits comparing categories, but rate of change suits tracking movement over time)
	• what variability means within a dataset and why understanding variability matters before drawing a conclusion from an average or total alone
	• that identifying a relationship between two or more variables requires interpretation, not just calculation
	• the relationship between data preparation, analytical methods and the reliability of conclusions.
	
	Learners should be able to analyse prepared datasets to identify patterns, relationships and trends.

2.3.2 Analytical outputs	Learners should know and understand: • what a summary is and how it can be used to condense a large amount of data down to its key points • what a comparison is and how it can be used to show how two or more things measure up against each other • what a trend is and how it can be used to show the general direction or pattern of data points over time • what an indicator is and how it can be used to signal a bigger picture.

DRAFT

© WJEC CBAC Ltd 2027.

	Learners should be able to: • draw reasoned conclusions from analysed data • ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations • review presented outputs to improve clarity, accessibility and relevance.

2.3.3 Interpretation and professional judgement in generating conclusions	Learners should know and understand:
	• how data quality, data limitations and analytical approach influence uncertainty and confidence in conclusions
	• how the following can influence the confidence of generating a conclusion, including:
	  • outliers
	  • sampling bias
	  • unrepresentative data
	  • sample size
	• the role of interpretation and professional judgement in transforming analytical results into meaningful conclusions
	• what correlation means and how this is used to generate conclusions
	• the risks of mistaking correlation for a meaningful relationship
	• the difference between correlation and meaningful relationships when transforming analytical results into meaningful conclusions.
	
	Given an analytical result, learners should be able to:
	• communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences
	• ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations
	• review presented outputs to improve clarity, accessibility and relevance.

Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.5.1 Communication in technical support • 1.5.2 Adapting communication for users • 1.5.3 Professional, ethical and responsible communication	

DRAFT

© WJEC CBAC Ltd 2027.

2.4 Automated and AI-enabled analysis

This topic introduces the use of automated and AI-enabled tools to support data analysis and insight generation. Learners develop knowledge and understanding of how AI systems can be used to identify patterns, generate analytical outputs and support decision making, alongside the benefits, limitations and risks associated with their use. The topic emphasises the importance of responsible and effective use of AI, including critical evaluation of AI-generated outputs, awareness of bias and uncertainty, appropriate governance and data protection practices, and the transparent presentation of insights using automated visualisation tools.

In this topic learners will gain knowledge, understanding and skills in the following areas:
2.4.1 AI systems
2.4.2 AI-enabled analytical systems
2.4.3 Limitations of AI-enabled analysis
2.4.4 Governance and data protection with AI-enabled analysis
2.4.5 Automated visualisation tools

Across section 1.4 learners should apply principles of responsible AI use, including awareness of limitations and bias, effective prompt design, human oversight, transparency of AI involvement, and critical evaluation of AI-generated outputs.

Section	Amplification

2.4.1
AI systems
	Learners should know and understand:
	• the role of AI in different contexts
	• the benefits of using AI
	• human oversight and responsible use including:
	  • the importance of human oversight in AI use
	  • the importance of critical thinking when using AI
	  • verification and validation practices
	  • appropriate and inappropriate uses of AI
	• AI harms and social impact
	• privacy and security considerations when using AI, such as:
	  • what counts as personal data and sensitive information in the context of AI use
	  • how AI systems use data
	  • Risks associated with oversharing information with AI tools
	  • Cyber security implications of AI
	  • Data protection principles relevant to AI use
	• bias, transparency and ethical AI principles, including:
	  • sources of bias in AI systems
	  • the importance of transparency and explainability in AI systems
	  • ethical AI principles such as:
	  • fairness
	  • accountability
	  • transparency
	  • human agency.

2.4.2 AI-enabled analytical systems	Learners should know and understand: • the types of automated and AI-enabled analytical systems and how they are used in different contexts • AI-enabled analytical systems can support insight generation by producing a suggestion, not a verified fact

DRAFT

© WJEC CBAC Ltd 2027.

	• why AI-generated outputs still need to be interpreted critically, such as:
	  • systems don't understand context, only patterns in numbers
	  • small or unusual samples can produce false patterns
	  • the training data shapes and limits what the system can see and do
	  • outputs are often presented with unearned confidence
	• why a specific AI-generated insight should or shouldn't be trusted before it's used to support a conclusion.
	
	Learners should be able to:
	• use an automated or AI-enabled analytical tool to help identify patterns or generate insights from a dataset
	• explain why a specific AI-generated insight should or shouldn't be trusted before it's used to support a conclusion.

2.4.3 Limitations of AI-enabled analysis	Learners should know and understand:
	• that datasets used in automated or AI-enabled analysis have limitations, such as:
	  • coverage and completeness
	  • training data
	  • AI model variation
	• there are potential sources of bias in the collection, preparation, processing and interpretation of data used in automated or AI-enabled analysis, such as:
	  • collection stage preparation stage
	  • processing stage limitations of datasets used in automated and AI-enabled analysis and potential sources of bias in data collection, preparation, processing and when drawing conclusions.
	
	Learners should be able to:
	• identify limitations in a range of datasets that could affect how trustworthy an automated or AI-enabled analysis of it would be
	• check for potential bias introduced in the collection and preparation stage of AI-enabled analysis and assess it potential impact
	• consider how a dataset's characteristics could bias how an AI system processes it)
	• reflect on whether their own interpretation of an automated output might be influenced by what they expected or wanted to see.

2.4.4 Governance and data protection with AI-enabled analysis	Learners should know and understand:
	• there is no single, common framework of laws, regulatory guidance or ethical standards governing AI systems across countries or jurisdictions. Each country applies its own, shaped by factors such as:
	  • which systems are used
	  • where they are used
	  • who uses them,
	  • what data they can access and control
	• what lawful and appropriate use of data means when using AI for analysis (for example only using data for the purpose it was collected for and having a proper basis for using it at all)
	• what protection of personal and sensitive information requires in an AI context (for example anonymising data before feeding it into a system and restricting who can access it)

DRAFT

© WJEC CBAC Ltd 2027.

	• why transparency and explainability when presenting insights of automated outputs matter for governance specifically • what accountability and human oversight means in practice (for example a named person remains responsible for checking and signing off an AI-generated output, rather than the system being left to act unchecked) • what accuracy, fairness and bias mitigation requires.

2.4.5 Automated visualisation tools	Learners should know and understand:
	• that automated visualisation tools make design choices automatically on a user's behalf that may influence the accessibility and interpretation of findings including:
	  • scale
	  • proportion
	  • representation
	• that leaving assumptions, limitations and confidence unexplained when presenting an automated output can produce consequences. such as:
	  • decisions being made on a false sense of certainty
	  • resources being misallocated based on a result
	  • mistakes being harder to trace back to their source once something goes wrong
	  • bias or unfairness in the data going unchallenged
	• that an automated output can be entirely accurate in its calculation and still be misleading in its presentation, if the assumptions, limitations and confidence behind it aren't made visible
	• the importance of transparency when using AI tools and for AI-supported insights, more than for a manually produced one
	• that failing to disclose AI involvement, or disclosing it vaguely, can mislead a viewer.
	
	Learners should be able to:
	• select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately
	• make changes to a visualisation tool's settings where they would otherwise mislead
	• explain how a chosen visualisation could influence a viewer's interpretation of the findings.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.8.1 Artificial intelligence fundamentals
- 1.8.3 AI capabilities, limitations and decision making
- 1.8.4 Prompts, structured inputs and generated outputs
- 1.8.5 Ethical, legal, social and sustainable digital practice

DRAFT

© WJEC CBAC Ltd 2027.

2.5. Data ethics, privacy, inclusion and sustainability

This topic introduces the ethical, legal and sustainable principles that underpin the responsible use of data throughout its lifecycle. Learners develop knowledge and understanding of data privacy, confidentiality and appropriate data use, alongside the importance of identifying and addressing bias, ensuring inclusivity, and presenting analytical findings fairly and transparently. The topic emphasises the responsibilities associated with handling data, the potential impacts of data-related decisions on individuals and organisations, and the importance of adopting sustainable practices when preparing, storing and sharing data.

In this topic learners will gain knowledge, understanding and skills in the following areas:
2.5.1 Data privacy, confidentiality and responsible use
2.5.2 Inclusive and unbiased data handling
2.5.3 Sustainability in data practice

Section	Amplification

2.5.1 Data privacy, confidentiality and responsible use	Learners should know and understand:
	• that there are laws, regulatory policies and procedures that govern the collection, storage and retention of data in the UK
	• the principles that underpin regulation
	• other countries have their own equivalent policies
	• that organisations in the UK can have their own internal policies governing collection, storage and retention of data but these must meet the legal minimum set by UK law
	• how access permissions and authorised use are applied to control who can view or use data, and for what purpose
	• how and why anonymisation is used to protect personal or sensitive information before data is shared, analysed or presented
	• that policies apply all the way through a piece of analytical work, including:
	  • collection
	  • storage
	  • preparation
	  • analysis
	  • presentation
	• that failing to follow these policies has real consequences for a range of stakeholders such as:
	  • customers
	  • employees
	  • partner organisations or third parties
	  • society or communities.
	
	Learners should be able to:
	• apply anonymisation to protect personal or sensitive information before sharing, analysing or presenting data
	• apply privacy and confidentiality considerations at every stage of a task, not only at the point of data collection
	• identify where a privacy, confidentiality or data-use policy has been breached or is at risk of being breached and know what to do about it.

DRAFT

© WJEC CBAC Ltd 2027.

2.5.2 Inclusive and unbiased data handling	Learners should know and understand:
	• what bias, incompleteness and lack of representativeness each mean in the context of using datasets
	  • the impacts of bias, incompleteness and lack of representativeness can have on both the outcomes of an analysis and how those outcomes are interpreted
	• principles of inclusive and unbiased data handling that support fair, accurate and responsible interpretation of analytical findings, such as:
	  • using consistent methods for collecting and processing data
	  • applying the same criteria to all groups
	  • protecting privacy and confidentiality
	  • data handling practices do not disadvantage individuals or groups
	• potential sources of bias in data collection, analysis and representation, such as:
	  • incomplete sampling
	  • low response rates
	  • inaccurate or outdated data
	  • selective use of data
	• the importance of considering completeness and representativeness of datasets such as:
	  • ensuring sufficient data has been collected
	  • identifying missing or duplicated records
	  • recognising underrepresented groups
	  • understanding how gaps in data may affect the reliability of conclusions
	• how misleading comparisons and visualisations can affect interpretation such as:
	  • the use of inappropriate scales
	  • selective time periods
	  • unsuitable chart types
	  • comparisons that do not account for differences in context, which may lead audiences to draw inaccurate conclusions
	• the importance of presenting findings objectively and transparently, including:
	  • reporting results accurately
	  • distinguishing between evidence and opinion
	  • acknowledging assumptions
	  • data quality issues and limitations
	• the need to consider the needs of diverse users and audiences including differing levels of technical knowledge, language and communication needs, accessibility requirements, cultural considerations, and the purpose for which information will be used when selecting content and presentation methods.
	
	Learners should be able to:
	• interpret analytical findings and consider potential sources of bias and limitation in the data
	• ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations
	• communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences.

DRAFT

© WJEC CBAC Ltd 2027.

2.5.3 Sustainability in data practice	Learners should know and understand:
	• approaches in sustainability when preparing, storing and sharing data such as:
	  • data preparation- green data centres, right-sizing compute, query optimisation
	  • data storage- compression, deduplication, lifecycle tiers
	  • data sharing- access over copying, on-demand generation, edge caching.

Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.8.4 Prompts, structured inputs and generated outputs • 1.8.5 Ethical, legal, social and sustainable digital practice	

DRAFT

© WJEC CBAC Ltd 2027.

2.6 Presenting and communicating

This topic introduces the principles of presenting and communicating analytical findings to support decision making in workplace contexts. Learners develop knowledge and understanding of how audience needs, workplace requirements and the intended purpose influence the selection and design of presentation formats. The topic emphasises the clear, accurate and accessible communication of data, insights and conclusions, ensuring that information is presented transparently and effectively for both technical and non-technical audiences.

In this topic learners will gain knowledge, understanding and skills in the following areas:
2.6.1 Presenting and communicating

Section	Amplification

2.6.1 Presenting and communicating	Learners should know and understand:
	• how workplace setting, audience needs and decision-making purpose influences presentation formats, such as:
	  • accessibility features
	  • workplace constraints (software and hardware availability)
	  • interactive elements
	  • level of detail
	  • purpose of presentation (informing, monitoring or supporting decisions)
	• the principles of visual communication such as:
	  • accurate representation
	  • transparent design
	  • proportionate scaling
	• inclusive and accessible presentation practices
	• that presentations may need to be adapted for different audiences to support equal understanding and accessibility.
	
	Learners should be able to:
	• apply different presentation formats, taking into consideration workplace setting, audience needs and decision-making purpose
	• justify why a chosen presentation format suits the specific setting, audience and purpose involved
	• select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately
	• ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations
	• communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences
	• review presented outputs to improve clarity, accessibility and relevance
	apply inclusive and accessible practices to support different audiences' understanding.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.5.1 Communication in technical support
- 1.5.2 Adapting communication for users
- 1.5.3 Professional, ethical and responsible communication

DRAFT

© WJEC CBAC Ltd 2027.

Transferrable skills			
	Analysing when identifying patterns, relationships and trends within datasets and interpreting findings	Decision making when selecting analytical approaches and drawing justified conclusions	Communicating when presenting insights clearly to technical and non-technical audiences
2.1.1	✓	✓	✓
2.1.2	✓	✓	
2.1.3	✓	✓	
2.2.1	✓	✓	✓
2.2.2	✓	✓	
2.3.1	✓	✓	
2.3.2	✓	✓	✓
2.3.3	✓	✓	✓
2.4.1		✓	
2.4.2	✓	✓	
2.4.3	✓	✓	
2.4.4		✓	
2.4.5	✓	✓	✓
2.5.1	✓	✓	
2.5.2	✓	✓	✓
2.5.3		✓	
2.6.1		✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 3 Cyber Security and Secure Digital Systems

GLH	80
Overview of content area	This content area develops the knowledge, understanding and skills required to protect digital systems, networks, devices and data from security threats. Learners explore the principles of cyber security and the measures used to maintain the confidentiality, integrity and availability of digital information. They develop an understanding of how secure digital systems are designed, implemented, monitored and maintained to protect individuals, organisations and wider digital infrastructures. The content area enables learners to understand common cyber threats, vulnerabilities and attack methods, as well as the security controls used to prevent, detect and respond to cyber incidents. Learners also develop an appreciation of the legal, ethical and professional responsibilities associated with cyber security, including the importance of managing risk, safeguarding data and promoting secure working practices in a range of digital environments. The knowledge and understanding developed through this content area builds upon the core knowledge and understanding established in Content Area 1. Together, these content areas provide the conceptual foundation that underpins achievement across the qualification. Where concepts are reflected across both content areas, the core knowledge and understanding from Content Area 1 defines what learners are expected to know and understand, while the knowledge and understanding in this content area provides opportunities to apply that knowledge in context. Through engagement with the activities, scenarios and tasks contained within the Work-Related Purposes, learners are expected to apply, demonstrate and extend their knowledge and understanding in authentic vocational contexts. These experiences provide opportunities for learners to further develop and deepen their core knowledge and understanding while identifying risks, implementing security measures, responding to security challenges and supporting the development of secure digital systems.
Topics	3.1 Access control, acceptable use and secure system practice 3.2 Cyber security threats, vulnerabilities and protective response 3.3 Monitoring and interpreting system information for security indicators
Summary of assessment	Non-exam assessment Assessment 4: Cyber Security and Secure Digital Systems • 18 hours • Set by WJEC, centre marked, moderated by WJEC • 80 marks.

DRAFT

© WJEC CBAC Ltd 2027.

Resources required for assessment	Candidates will require access to suitable digital devices, software, virtualised environments and assessment resource files that enable them to assess organisational security practices, implement security controls, analyse security information, evaluate AI-enabled cyber defence outputs and produce incident response documentation. Centres must install and configure Oracle VirtualBox prior to delivery of the assessment. WJEC will provide detailed installation and set-up guidance for centres. Centres are responsible for ensuring that all hardware, software and assessment resources required to complete the assessment are available throughout the supervised assessment period.

Content

3.1 Access control, acceptable use and secure system practice

This topic introduces the principles and practices used to protect digital systems, data and services from unauthorised access and misuse. Learners develop knowledge and understanding of the policies, procedures and controls that support secure system use, including acceptable use, data handling, incident reporting, authentication and access control. The topic emphasises the application of security measures to manage access, protect information, support secure system operation and promote responsible and compliant digital practice.

In this topic learners will gain knowledge, understanding and skills in the following areas:
3.1.1 Policies guiding secure practice
3.1.2 Applying access control and authentication measures to protect digital systems

Section	Amplification

3.1.1 Policies guiding secure practice	Learners should know and understand:
	• policies relating to acceptable use, access control, data handling and incident reporting, and their role in guiding secure practice
	• the scope of and requirements of an acceptable use policy, such as:
	  • permitted use
	  • access management
	  • device and services security
	  • user authentication
	  • consequences of misuse
	• the scope of a data handling policy, such as:
	  • secure storage
	  • access controls
	  • data sharing, disposal and retention
	• the scope and requirements of incident reporting policy, such as:
	  • what counts as an incident
	  • how to report an incident
	  • timeframe for reporting
	  • escalation process

© WJEC CBAC Ltd 2027.

	Learners should be able to: • identify when a situation should be reported as a suspected security incident and follow the correct reporting/escalation route • identify how a described action or scenario breaches one of these policies and explain which policy area is affected.

3.1.2 Applying access control and authentication measures to protect digital systems	Learners should know and understand:
	• the different methods of authentication used to verify a user's identity, such as:
	  • one-time passcodes
	  • multi-factor authentication
	  • biometrics
	• common uses of authentication in a variety of contexts, such as:
	  • logging into a company laptop using a username and password
	  • entering a password and then a one-time code sent to a mobile phone to access financial information and services
	  • unlocking a phone using Face ID
	• the purpose of access control measures and their use in different contexts, such as:
	  • role based access
	  • time limited or conditional access
	  • physical access control linked to digital permissions
	  • edit and read permissions
	• the purpose of using update and patch procedures
	• the role of operating systems, user accounts and access controls in enabling secure and effective system use
	• the types of data protection measures used in a variety of contexts, such as:
	  • encryption
	  • secure storage
	  • controlling how data is transmitted
	  • backup procedures
	• the relationship between authentication strength, usability and security risk
	• the principle of least privilege
	• the dependency relationships between configuration settings and system behaviour.
	
	Learners should be able to apply:
	• authentication requirements, access controls, update procedures and data protection measures to digital systems
	• configuration actions relating to user accounts, permissions and security settings in line with defined security procedures
	• procedures for secure access, authentication and system use.

© WJEC CBAC Ltd 2027.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.1.2 The role of the operating system in digital systems
- 1.1.3 Users, authentication and access control
- 1.2.1 Configuration requirements
- 1.2.2 Configuration dependencies and consistency
- 1.2.3 Configuration for workplace and user requirements
- 1.2.4 Configuration risks and consequences
- 1.4.2 Interpreting system behaviour
- 1.4.3 Structured fault diagnosis and resolution
- 1.4.4 Consequences and responsible fault management

DRAFT

© WJEC CBAC Ltd 2027.

3.2 Cyber security threats, vulnerabilities and protective response

This topic introduces the nature of cyber security threats, vulnerabilities and incidents, and the measures used to protect digital systems, services and data. Learners develop knowledge and understanding of common cyber threats, threat actors and protective controls, alongside the role of vulnerability management and incident response in maintaining cyber resilience. The topic emphasises the importance of identifying and responding to security risks, understanding how technical controls and user behaviour influence system vulnerability, and recognising the operational, financial and reputational impacts that cyber incidents can have on individuals and organisations.

In this topic learners will gain knowledge, understanding and skills in the following areas:
3.2.1 Cyber security threats and protection methods
3.2.2 Vulnerability management
3.2.3 The impacts and implications of cyber threats

Section	Amplification

3.2.1 Cyber security threats and protection methods	Learners should know and understand:
	• a range of common cyber security threats, including:
	  • phishing
	  • social engineering
	  • malware
	  • ransomware
	  • unauthorised access attempts
	  • suspicious network behaviour
	  • data loss incidents
	  • Exposed network services
	  • Insecure default configurations
	• that AI can be used to generate a range of cyber-attacks, such as:
	  • voice cloning
	  • deepfake video or images
	  • generate or adapt malware
	  • automate and scale social engineering attacks
	• that there are a range of threat actors, each with distinct motivations and objectives for carrying out cyber incidents, such as:
	  • nation states (for example countries targeting critical national infrastructure)
	  • organised crime (for example groups stealing data or money for profit)
	  • insiders (for example employees or supply chain personal who misuse access)
	• a range of protection methods against cyber security threats, such as:
	  • firewalls
	  • software updates and patching
	  • encryption
	  • antivirus software
	• that AI is being used to defend against cyber-attacks, such as:
	  • anomaly detection
	  • faster triage
	  • predictive and threat modelling.

DRAFT

© WJEC CBAC Ltd 2027.

	Learners should be able to: • select and apply protective actions to systems in response to identified risks and system information • develop an incident response plan to communicate potential security concerns clearly to others • handle security-related information in line with policies and procedures for privacy and confidentiality • select and apply appropriate actions to restore a systems functionality.

3.2.2 Vulnerability management	Learners should know and understand:
	• the role of security controls, and how user behaviour can affect their effectiveness.
	• that system vulnerabilities can arise from weaknesses in the controls themselves, from how users behave, or from the interaction between the two
	• that a user's behaviour can change over time, which changes the level of vulnerability even if the technical controls stay the same
	• the importance of vulnerability management
	• the purpose and application of an incident response plan in managing a cyber security incident, covering stages such as:
	  • analysis
	  • containment
	  • mitigation
	  • remediation/eradication
	  • recovery
	  • post incident review.
	
	Learners should be able to:
	• identify the security controls present
	• identify user behaviours in a scenario that increase or reduce vulnerability
	• explain how a specific combination of security controls and user behaviour has created a vulnerability
	• assess how security controls and user behaviour combine to create or reduce system vulnerability
	• recommend a change to controls, behaviour, or both, to reduce an identified vulnerability or risk
	• communicate potential security concerns clearly to others
	• develop, evaluate an incident response plan for a given context.

3.2.3 The impacts and implications of cyber threats	Learners should know and understand:
	• that cyber threats can have a range of impacts, such as:
	  • financial loss
	  • reputational damage
	  • service downtime
	• the implications of different types of cyber threats and the impact of delayed identification and escalation, such as:
	  • extended system downtime
	  • higher recovery costs
	  • impact third parties in a supply chain.
	
	Learners should be able to select and apply protective actions in response to identified risks and system information.

© WJEC CBAC Ltd 2027.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.2.1 Configuration requirements
- 1.2.2 Configuration dependencies and consistency
- 1.2.3 Configuration for workplace and user requirements
- 1.2.4 Configuration risks and consequences
- 1.4.2 Interpreting system behaviour
- 1.4.3 Structured fault diagnosis and resolution
- 1.4.4 Consequences and responsible fault management

DRAFT

© WJEC CBAC Ltd 2027.

3.3 Monitoring and interpreting system information for security indicators

This topic introduces the principles of monitoring and interpreting system information to identify, assess and respond to potential cyber security concerns. Learners develop knowledge and understanding of how logs, alerts, account activity and other security-related information can be used to detect unusual behaviour and indicators of compromise, alongside the role of automated and AI-enabled detection systems in supporting cyber security monitoring. The topic emphasises the importance of applying professional judgement when interpreting system information, validating automated outputs, and recording, handling and escalating security concerns in line with secure, responsible and organisationally defined procedures.

In this topic learners will gain knowledge, understanding and skills in the following areas:
3.3.1 Security monitoring
3.3.2 Automated and AI-enabled detection systems
3.3.3 Recording band escalating security concerns

Section	Amplification

3.3.1 Security monitoring	Learners should know and understand:
	• methods to identify a potential cyber security concern, including:
	  • system logs
	  • alert notifications
	  • account activity records
	  • using multiple indicators
	• the difference between normal system variation and anomalous behaviour when identifying a potential cyber security concern
	• how the interpretation of system activity and security-related information can influence whether a concern is genuine and the need for professional judgement
	• that baseline system behaviour can be used as a reference point against which deviations and potential threats are identified and that a baseline can change over time and needs to be reviewed.
	
	Learners should be able to:
	• identify indicators of potential cyber security concerns within logs, alerts or account activity records, including correlation of multiple indicators and distinguishing normal system variation from anomalous behaviour
	• explain how these indicators could influence a system, such as:
	  • slow response times
	  • repeated errors
	  • failed updates
	  • connectivity interruptions
	• record observations clearly and accurately
	• recognise signs of unexpected and anomalous system activity
	• use log files, monitoring dashboards and system alerts to view and interpret security-related information
	• apply professional judgement to interpret the relationship between system activity, security-related information and potential cyber security concerns
	• escalate potential cyber security concerns in line with security procedures
	• communicate potential security concerns clearly to others

DRAFT

© WJEC CBAC Ltd 2027.

	• review security-related information to identify slow response times, repeated errors, failed updates and connectivity interruptions, and what these indicate about system quality.

3.3.2 Automated and AI-enabled detection systems	Learners should know and understand:
	• the role and limitations of automated and AI-enabled detection in identifying potential cyber security concerns and the need to accurately interpret, validate and act on system information and automated outputs, including:
	  • false positives
	  • misinterpretation of automated alerts.
	
	Learners should be able to:
	• assess whether a flagged alert from an automated or AI-enabled detection system is likely a false positive or a genuine concern, based on the available information
	• identify a limitation of a specific automated/AI-enabled detection system that could affect its reliability in a scenario
	• validate an automated system's output against other available information before acting on it
	• decide and justify an appropriate action in response to a validated automated/AI-enabled detection output.

3.3.3 Recording and escalating security concerns	Learners should know and understand:
	• the importance of policies and procedures relating to privacy, confidentiality and responsible handling of security-related information for:
	  • storing security-related information securely
	  • restricting access to authorised users
	  • transmitting information appropriately
	  • reporting and escalating concerns through defined procedures
	• the importance of energy efficiency in a cyber security context
	• the purpose and benefits of data retention management in cyber security
	• principles of safe, secure and responsible practice when diagnosing and resolving faults
	• the purpose and benefits of the secure by design principle in securing systems and data, such as:
	  • establish the context
	  • making compromise difficult
	  • making disruption difficult
	  • making compromise detection easier
	  • reducing the impact of compromise
	• the purpose and benefits of secure device lifecycle practice, such as:
	  • controlling assets
	  • embedding security
	  • standardising practices.
	
	Learners should be able to:
	• escalate potential cyber security concerns in line with security procedures
	• select and apply protective actions to systems in response to identified risks and system information.

DRAFT

© WJEC CBAC Ltd 2027.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.4.4 Consequences and responsible fault management
- 1.8.1 Artificial intelligence fundamentals
- 1.8.3 AI capabilities, limitations and decision making
- 1.8.4 Prompts, structured inputs and generated outputs
- 1.8.5 Ethical, legal, social and sustainable digital practice

DRAFT

© WJEC CBAC Ltd 2027.

Transferrable skills			
	Investigative skills, demonstrated through interpreting system information and monitoring outputs to identify unusual or anomalous behaviour	Decision making when selecting actions and escalation routes in line with defined security procedures	Communicating when reporting observations and potential concerns clearly
3.1.1		✓	✓
3.1.2		✓	
3.2.1	✓	✓	✓
3.2.2	✓	✓	✓
3.2.3	✓	✓	
3.3.1	✓	✓	✓
3.3.2	✓	✓	
3.3.3		✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 4 Digital Systems Configuration, Testing and Support (Optional route)

GLH	80
Overview of content area	This content area develops the knowledge, understanding and skills required to configure, test, maintain and support digital systems. Learners explore how hardware, software and network components are installed, configured and managed to meet user and organisational requirements. They develop an understanding of the processes and practices used to ensure that digital systems operate effectively, efficiently and securely. The content area enables learners to understand how digital systems are tested, monitored and maintained to identify and resolve issues, optimise performance and support users. Learners also develop an appreciation of the importance of documentation, troubleshooting, quality assurance and user support in maintaining reliable digital services and ensuring that systems continue to meet operational needs. The knowledge and understanding developed through this content area builds upon the core knowledge and understanding established in Content Area 1. Together, these content areas provide the conceptual foundation that underpins achievement across the qualification. Where concepts are reflected across both content areas, the core knowledge and understanding from Content Area 1 defines what learners are expected to know and understand, while the knowledge and understanding in this content area provides opportunities to apply that knowledge in context. Through engagement with the activities, scenarios and tasks contained within the Work-Related Purposes, learners are expected to apply, demonstrate and extend their knowledge and understanding in authentic vocational contexts. These experiences provide opportunities for learners to further develop and deepen their core knowledge and understanding while configuring systems, testing solutions, resolving technical issues and supporting users to ensure digital systems remain effective, secure and fit for purpose.
Topics	4.1 Planning and preparing digital systems 4.2 Digital system configuration and management 4.3 Usability, accessibility and inclusive practice 4.4 Testing, validation and quality assurance 4.5 System monitoring, fault diagnosis and resolution
Summary of assessment	Non-exam assessment Assessment 5a: Digital Systems Configuration, Testing and Support • 15 hours • Set and marked by WJEC • 80 marks

© WJEC CBAC Ltd 2027.

Resources required for assessment	Candidates will require access to suitable digital devices, software, virtualised environments and assessment resource files that enable them to configure, maintain and optimise digital systems, implement system and user requirements, test functionality, troubleshoot issues, evaluate the effectiveness of implemented solutions and produce technical documentation. Centres must install and configure Oracle VirtualBox prior to delivery of the assessment. WJEC will provide detailed installation and set-up guidance for centres. Centres are responsible for ensuring that all hardware, software and assessment resources required to complete the assessment are available throughout the supervised assessment period.

Content

4.1 Planning and preparing digital systems

This topic introduces the principles of planning, configuring and preparing digital systems to meet defined user, organisational and technical requirements. Learners develop knowledge and understanding of how hardware, software, networking, storage and security considerations influence configuration decisions, alongside the use of appropriate tools and environments to safely implement, test and validate system configurations. The topic emphasises the importance of evaluating configuration choices against requirements, performance, security, sustainability and resource efficiency to ensure digital systems operate effectively, reliably and responsibly.

In this topic learners will gain knowledge, understanding and skills in the following areas:
4.1.1 Preparing and configuring digital systems
4.1.2 Testing and validating digital system configurations
4.1.3 Evaluating configuration decisions and system performance

Section	Amplification
4.1.1 Evaluating configuration decisions and system performance	Learners should know and understand: • how to apply knowledge of hardware, software, network infrastructure, data storage and user interfaces when selecting and implementing configuration settings within digital systems • the principles of configuring digital systems to manage users, access, connectivity, storage and security, ensuring systems operate securely and as intended and the importance of managing configuration consistently to maintain reliable, secure and predictable system behaviour • how to choose and apply configuration settings to meet operational requirements while balancing performance, usability, accessibility and security • how to evaluate technical, security, organisational and resource constraints and apply this understanding when making implementation decisions and designing collaborative solutions Learners should be able to: • interpret user and system requirements to determine configuration needs, including:

© WJEC CBAC Ltd 2027.

	• identifying required configuration settings • determining user access requirements • identifying connectivity, storage and security requirements • prepare and configure digital systems to meet defined needs, including: • applying configuration settings • configuring user access and permissions • configuring connectivity • configuring storage settings • configuring security settings.
4.1.2 Testing and validating digital system configurations	Learners should know and understand: • the role of configuration environments, such as: • controlled • non-live • simulated • training how these environments support: • safe testing of configuration changes • validation of configuration decisions • reduction of risk to live systems • development of configuration skills and procedures • the role of digital tools in supporting system preparation, configuration and checking activities, including tools used to: • prepare systems for implementation • apply and manage configuration settings • monitor and check configuration outcomes • validate that systems meet defined requirements • the role of system dependencies and component compatibility in ensuring reliable system operation, including: • hardware compatibility • software compatibility • operating system dependencies • network and service dependencies • security dependencies. Learners should be able to: • select and use appropriate digital tools to support preparation, configuration and validation activities • carry out configuration activities within controlled environments before implementation in operational systems, including: • testing configuration changes • validating configuration outcomes • identifying potential issues before deployment.
4.1.3 Evaluating configuration decisions and system performance	Learners should know and understand: • the impact of system configuration on performance efficiency and resource utilisation, such as processor, storage, network, security requirements, and energy consumption • environmental and sustainability considerations associated with system performance and the efficient use of digital resources, such as: • efficient use of network resources • efficient use of processing and memory resources

DRAFT

© WJEC CBAC Ltd 2027.

	• efficient use of storage resources • energy consumption • extending device lifespan and reducing electronic waste • reducing unnecessary resource utilisation. Learners should be able to make configuration decisions that balance performance, sustainability, ethical and legal considerations, organisational needs and efficient use of digital resources, including the responsible use of automated and AI-enabled systems and their outputs.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.1.1 Digital systems and their components
- 1.2.1 Configuration requirements
- 1.2.2 Configuration dependencies and consistency
- 1.2.3 Configuration for workplace and user requirements
- 1.3.1 Requirements and the purpose of testing
- 1.3.2 Test outcomes and evidence
- 1.3.3 Performance thresholds and system quality
- 1.3.4 Performance, usability and security trade-offs
- 1.3.5 Judging system readiness
- 1.6.2 Identifying and interpreting user needs
- 1.6.3 Translating needs into digital solution requirements
- 1.6.4 Constraints and inclusive decision making

DRAFT

© WJEC CBAC Ltd 2027.

4.2 Digital system configuration and management

This topic introduces the principles of configuring, securing and managing digital systems to ensure they operate effectively, reliably and in accordance with organisational requirements. Learners develop knowledge and understanding of access control, authentication, security management and secure configuration practices, alongside the policies and procedures that support data protection, privacy and compliance. The topic emphasises the importance of maintaining system integrity through responsible configuration, effective management of permissions and updates, and the application of security controls that protect systems, services and data from unauthorised access or modification.

In this topic learners will gain knowledge, understanding and skills in the following areas:
4.2.1 Access control and security management
4.2.2 Secure configuration and compliance
4.2.3 System integrity and protection

Section	Amplification

4.2.1 Access control and security management	Learners should know and understand:
	• how operating systems, user accounts and access controls are managed to support authentication, access permissions and the secure use of systems, services and resources
	• how configuration-related risks can arise from access permissions, authentication settings, software, network services and default configurations, and the potential impact of these risks on systems, services and users
	
	Learners should be able to:
	• adjust configuration settings relating to user access, connectivity, storage and security to support system functionality and accessibility
	• identify and correct configuration settings relating to user access, connectivity, storage and security that do not meet defined user requirements
	• apply routine checks to confirm readiness for use, including:
	  • user access and authentication
	  • connectivity and network access
	  • storage availability
	  • software updates
	  • security settings
	  • expected system functionality and performance.

4.2.2 Secure configuration and compliance	Learners should know and understand:
	• how policies relating to data protection, privacy and acceptable system use and their influence on configuration practice, including:
	  • access permissions and user account management
	  • secure configuration practices
	  • software update and patch management
	  • protection of personal and sensitive information
	  • privacy and confidentiality requirements
	  • acceptable use of systems, devices and services

DRAFT

© WJEC CBAC Ltd 2027.

	• how to implement secure, ethical and sustainable digital practices in line with legal and organisational requirements, including intellectual property rights, ownership, attribution, and the responsible use of automated and AI-enabled systems and their outputs • ethical, legal and sustainability considerations relevant to digital practice, including responsible use of automated and AI-enabled systems. Learners should be able to apply policies relating to secure configuration and data protection requirements, secure configuration, access permissions, software updates and protection of personal information.

4.2.3 System integrity and protection	Learners should know and understand:
	• the importance of maintaining system integrity through responsible updates, permissions and security settings.
	
	Learners should be able to:
	• maintain system integrity through:
	  • responsible configuration practices
	  • software and system updates
	  • management of permissions and access controls
	  • application of security settings and controls
	  • protection against unauthorised access and changes.

Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.1.2 The role of the operating system in digital systems • 1.1.3 Users, authentication and access control • 1.2.4 Configuration risks and consequences • 1.8.4 Prompts, structured inputs and generated outputs • 1.8.5 Ethical, legal, social and sustainable digital practice	

DRAFT

© WJEC CBAC Ltd 2027.

4.3 Usability, accessibility and inclusive practice

This topic introduces the principles of usability, accessibility and inclusive practice in the design, configuration and evaluation of digital systems. Learners develop knowledge and understanding of how digital solutions can be designed and tested to meet the needs of diverse users, including the role of accessibility, inclusive design and user feedback in improving user experience and reducing barriers to participation. The topic emphasises the importance of continuous improvement, effective communication, collaboration and documentation, and the application of professional, ethical and responsible practices when developing and supporting digital systems.

In this topic learners will gain knowledge, understanding and skills in the following areas:
4.3.1 Usability, accessibility and inclusive design
4.3.2 Inclusive testing and Continuous Improvement
4.3.3 Documentation, collaboration and communication

Section	Amplification

4.3.1 Usability, accessibility and inclusive design	Learners should know and understand:
	• the principles of usability and accessibility and their relevance to system performance, reliability and security for diverse users, including:
	  • accessibility of content and functionality
	  • adaptable presentation and access methods
	  • clear and consistent navigation
	  • compatibility with assistive technologies
	  • inclusive user testing
	  • intuitive interaction and interface design
	• how interface design, navigation structures and interaction patterns influence user effectiveness, user experience and accessibility.
	
	Learners should be able to:
	• assess system usability and accessibility against stated user needs, including:
	  • identifying barriers that affect usability or accessibility
	  • determining whether systems meet defined user requirements
	• consider the needs of diverse users evaluate systems against accessibility requirements and inclusive design principles, including:
	  • accessibility of content, features and functionality
	  • compatibility with assistive technologies, such as screen readers and alternative input devices
	  • effectiveness of navigation structures and interaction methods
	• consider how inclusive design supports the needs of a wide range of users.

4.3.2 Inclusive testing and continuous improvement	Learners should know and understand:
	• the contribution of inclusive and accessible testing practices to the development of reliable digital systems for diverse users, including:
	  • involving users with different needs and abilities
	  • identifying accessibility barriers
	  • identifying usability issues
	  • improving reliability and user experience
	  • supporting equitable access to digital systems

DRAFT

© WJEC CBAC Ltd 2027.

	• how to interpret user requirements, accessibility expectations and feedback to establish evaluation criteria and support the continuous improvement of digital solutions through iteration • the impact of responsible, inclusive and secure configuration practices on supporting diverse users, promoting accessibility and reducing barriers to digital participation. Learners should be able to consider how user feedback and testing outcomes can be used to identify improvements that support: • diverse users • accessibility and inclusion through appropriate testing and configuration activities.

4.3.3 Documentation, collaboration and communication	Learners should know and understand:
	• the role of clear documentation and communication in supporting accurate, consistent and effective system preparation and user support, including:
	  • technical documentation
	  • user documentation and guidance
	  • instructions and procedures
	  • communication of configuration decisions and outcomes
	• how collaboration supports the development, evaluation and continuous improvement of digital solutions through the contribution of different roles, perspectives and expertise, and the use of structured approaches to achieve effective and consistent outcomes
	• how ethical, professional and responsible practices support the creation, use and sharing of digital information and resources, including intellectual property rights, ownership, attribution, and the responsible use of digital and AI-enabled tools and their outputs.
	
	Learners should be able to:
	• produce clear technical and user documentation for configuration decisions, with consideration of accuracy and consistency of information
	• communicate technical information professionally while maintaining confidentiality and respecting privacy requirements and respond to user queries in line with workplace procedures.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.5.1 Communication in technical support
- 1.5.2 Adapting communication for users
- 1.5.3 Professional, ethical and responsible communication
- 1.6.1 Collaboration in digital work
- 1.6.2 Identifying and interpreting user needs
- 1.6.3 Translating needs into digital solution requirements
- 1.6.4 Constraints and inclusive decision making
- 1.8.4 Prompts, structured inputs and generated outputs
- 1.8.5 Ethical, legal, social and sustainable digital practice

DRAFT

© WJEC CBAC Ltd 2027.

4.4 Testing, validation and quality assurance

This topic introduces the principles of testing, validation and quality assurance used to evaluate the effectiveness, reliability and readiness of digital systems. Learners develop knowledge and understanding of how testing activities provide evidence that systems meet user, organisational and security requirements, alongside the role of quality assurance in supporting consistent performance and ongoing improvement. The topic emphasises the use of structured testing approaches, accurate documentation and reporting, and the application of digital, automated and AI-enabled tools to support the analysis, interpretation and communication of test outcomes.

In this topic learners will gain knowledge, understanding and skills in the following areas:
4.4.1 Testing principles and quality assurance
4.4.2 Test documentation and reporting
4.4.3 Digital, automated and AI-enabled testing tools

Section	Amplification

4.4.1 Testing principles and quality assurance	Learners should know and understand:
	• the purpose of testing digital systems
	• the role of quality assurance in maintaining system performance security and service reliability
	• categories of testing used in workplace contexts and the purpose of each when evaluating digital systems including:
	  • functionality testing
	  • performance testing
	  • usability testing
	  • accessibility testing
	  • security testing
	• how test outcomes provide evidence that systems:
	  • meet user requirements
	  • meet organisational requirements
	  • perform consistently and reliably
	  • are suitable for their intended purposes
	  • have robust security measures
	• how workplace policies, standards and compliance requirements influence testing activities, including:
	  • defining the scope of testing
	  • establishing acceptable outcomes
	  • setting quality assurance expectations
	• how requirements, testing outcomes and acceptance criteria inform decisions about system readiness, deployment and ongoing use, including balancing performance, usability and security requirements.
	
	Learners should be able to:
	• interpret user and system requirements to determine the scope and focus of testing activities, including:
	  • identifying features and functions to be tested
	  • determining success criteria and expected outcomes
	• evaluate test outcomes against requirements to determine whether:
	  • requirements have been met
	  • systems are ready for use
	  • further testing is required

DRAFT

© WJEC CBAC Ltd 2027.

	• configuration changes or corrective actions are needed before deployment • carry out structured tests to confirm system: • functionality • performance • stability • security-related behaviours.
4.4.2 Test documentation and reporting	Learners should know and understand: • the importance of recording and documenting test findings accurately and consistently including: • creating an audit trail • supporting review and accountability • enabling corrective actions and improvement decisions • supporting continuous improvement activities • ensuring accurate, consistent and effective system preparation. Learners should be able to: • record and compare test outcomes against requirements using: • accurate terminology • structured documentation formats • test records, logs and reports.
4.4.3 Digital, automated and AI-enabled testing tools	Learners should know and understand: • how contemporary digital tools support test planning, the identification of patterns in system behaviour and the analysis and communication of test findings such as: • test management tools • system monitoring tools • log analysis tools • data analysis and visualisation tools • how digital, automated and AI-enabled tools support testing activities by using prompts and structures to generate outputs, such as: • generating test cases • analysing large volumes of test data • identifying patterns and anomalies in system behaviour • summarising findings and recommending actions. Learners should be able to: • use digital and AI-enabled tools to support testing and analysis activities, such as: • test management tools • system monitoring tools • log analysis tools • data analysis and reporting tools • AI-enabled tools to support analysis and identification of patterns in test data.

DRAFT

© WJEC CBAC Ltd 2027.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.3.1 Requirements and the purpose of testing
- 1.3.2 Test outcomes and evidence
- 1.3.3 Performance thresholds and system quality
- 1.3.4 Performance, usability and security trade-offs
- 1.3.5 Judging system readiness
- 1.8.4 Prompts, structured inputs and generated outputs
- 1.8.5 Ethical, legal, social and sustainable digital practice

DRAFT

© WJEC CBAC Ltd 2027.

4.5 System monitoring, fault diagnosis and resolution

This topic introduces the principles of monitoring, diagnosing and resolving faults within digital systems to maintain effective, secure and reliable operation. Learners develop knowledge and understanding of how system behaviour, logs, alerts, diagnostic information and performance indicators can be used to identify issues, investigate causes and support fault resolution. The topic emphasises the use of structured troubleshooting approaches, effective technical communication and documentation, and the appropriate use of digital and AI-enabled diagnostic tools, while recognising the importance of professional judgement, human oversight and responsible practice when supporting users and services.

In this topic learners will gain knowledge, understanding and skills in the following areas:
4.5.1 Monitoring system behaviour, fault identification and resolution
4.5.2 Technical communication and diagnostic technologies

Section	Amplification

4.5.1 Monitoring system behaviour, fault identification and resolution	Learners should know and understand:
	• methods used to assess system behaviour through comparison of observed outputs with expected outcomes, including:
	• comparing actual results with expected results
	• identifying deviations from expected performance
	• checking whether systems meet defined requirements
	• determining whether corrective action is required
	• how the use of system logs, alerts, diagnostic information and performance indicators are used to identify issues, monitor system behaviour and support fault diagnosis, such as:
	  • system logs
	  • event logs
	  • error messages
	  • alerts and notifications
	• how to identify patterns and recurring issues
	• how hardware, software, network and user-related factors can contribute to technical faults in digital systems, and how system behaviour can be interpreted against expected outcomes to support fault identification and resolution
	• how structured diagnostic and troubleshooting approaches are applied to identify, investigate and resolve technical faults, using system information, diagnostic tools and logical processes to support accurate decision making, escalation and restoration activities
	• how to apply safe, secure and responsible practices when diagnosing and resolving faults, including the protection of personal and sensitive information, appropriate use of authorised access, and consideration of the impact of actions on users, services and organisations
	• the impact of performance, reliability and security-related issues on users, productivity and service continuity.
	
	Learners should be able to:
	• review system behaviour and outputs to identify deviations from expected outcomes by:
	• comparing observed outputs with expected results
	• identifying unusual system behaviour

DRAFT

© WJEC CBAC Ltd 2027.

	• recognising indicators of faults and performance issues
	• interpret evidence gathered from logs, alerts, diagnostics and performance information when assessing system behaviour
	• apply structured fault-finding approaches to investigate faults and determine likely causes, such as:
	  • gathering relevant evidence
	  • identifying possible causes
	  • testing potential solutions
	  • confirming the effectiveness of corrective actions
	• interpret evidence gathered from logs, alerts, diagnostics and performance information when assessing system behaviour
	• make informed decisions about fault resolution, escalation and further testing activities.

4.5.2 Technical communication and diagnostic technologies	Learners should know and understand:
	• how to gather, interpret and communicate technical information effectively to support fault resolution, informed decision making and service delivery
	• how communication approaches influence clarity, efficiency and user experience, and how they can be adapted to meet diverse user needs, workplace requirements and support activities
	• the role of digital tools and AI-enabled systems in supporting monitoring and diagnosis
	• the role of AI-enabled tools to identify trends, anomalies and recurring issues
	• how automated and AI-enabled monitoring and diagnostic tools are not always reliable with consideration of various factors, such as:
	  • bias
	  • the risk of false positives
	  • inaccurate outputs
	  • the need for human oversight to ensure reliability.
	
	Learners should be able to:
	communicate and document technical findings appropriately to users and stakeholders, supporting accurate, consistent and effective fault resolution and user support.

Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.4.1 Nature and causes of technical faults • 1.4.2 Interpreting system behaviour • 1.4.3 Structured fault diagnosis and resolution • 1.4.4 Consequences and responsible fault management • 1.5.1 Communication in technical support • 1.5.2 Adapting communication for users • 1.5.3 Professional, ethical and responsible communication	

© WJEC CBAC Ltd 2027.

Transferrable skills

	Analysing when interpreting user requirements, system information and system behaviour	Decision making when selecting configuration actions in line with defined requirements	Communicating when explaining configuration outcomes clearly
4.1.1	✓	✓	
4.1.2		✓	
4.1.3			
4.2.1	✓	✓	
4.2.2		✓	
4.2.3		✓	
4.3.1	✓		
4.3.2			
4.3.3			✓
4.4.1	✓	✓	
4.4.2	✓		✓
4.4.3	✓		
4.5.1	✓		✓
4.5.2	✓		✓

Work-related behaviours

	Perceptive when interpreting user requirements, system behaviour and data outputs to identify relevant issues or patterns	Attention to detail when configuring systems, reviewing system information and preparing or analysing data	Focussed when completing structured tasks such as testing, analysis and solution design within defined requirements	Respectful in interactions with users and colleagues, particularly when handling technical issues or responding to queries	Responsive when addressing system issues, user needs or emerging risks, including appropriate escalation where required
4.1.1	✓	✓	✓		

DRAFT

© WJEC CBAC Ltd 2027.

4.1.2	✓	✓	✓		
4.1.3		✓	✓		
4.2.1	✓	✓	✓	✓	✓
4.2.2		✓	✓		
4.2.3	✓	✓	✓	✓	✓
4.3.1	✓	✓	✓	✓	
4.3.2	✓	✓	✓	✓	
4.3.3		✓	✓	✓	✓
4.4.1	✓	✓	✓		✓
4.4.2	✓	✓	✓		
4.4.3	✓	✓	✓		✓
4.5.1	✓	✓	✓		✓
4.5.2	✓	✓	✓	✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

Content Area 5 Digital Solution Design and Development (Optional route)

GLH	80
Overview of content area	This content area develops the knowledge, understanding and skills required to design, develop and refine digital solutions that meet identified user and organisational needs. Learners explore the processes involved in planning, creating and evaluating digital products and services, including the use of appropriate tools, technologies and development approaches. They develop an understanding of how requirements are gathered, interpreted and translated into effective digital solutions. The content area enables learners to understand the principles of solution design, development and evaluation, including the importance of usability, functionality, accessibility and maintainability. Learners also develop an appreciation of iterative development processes, testing and refinement, and the role of user feedback in ensuring that digital solutions are fit for purpose and meet stakeholder requirements. The knowledge and understanding developed through this content area builds upon the core knowledge and understanding established in Content Area 1. Together, these content areas provide the conceptual foundation that underpins achievement across the qualification. Where concepts are reflected across both content areas, the core knowledge and understanding from Content Area 1 defines what learners are expected to know and understand, while the knowledge and understanding in this content area provides opportunities to apply that knowledge in context. Through engagement with the activities, scenarios and tasks contained within the Work-Related Purposes, learners are expected to apply, demonstrate and extend their knowledge and understanding in authentic vocational contexts. These experiences provide opportunities for learners to further develop and deepen their Core knowledge and understanding while designing, developing, testing, evaluating and refining digital solutions to address user and organisational needs.
Topics	5.1 User requirements, analysis and solution planning 5.2 Analyse, design and communicate digital solutions 5.3 Prototyping and development approaches 5.4 User-centred, secure and responsible digital solution design 5.5 Analyse, design and communicate digital solutions
Summary of assessment	Assessment 5b: Digital Solution Design and Development • 15 hours • Set and marked by WJEC • 80 marks

DRAFT

© WJEC CBAC Ltd 2027.

Resources required for assessment	Candidates will require access to suitable digital devices, software development tools and assessment resource files that enable them to analyse organisational and user requirements, design digital solutions, develop and test prototype applications, evaluate AI-generated design suggestions, refine solutions based on feedback and produce technical and user documentation. Centres must provide access to the software and tools required to design, develop, test and evaluate prototype digital solutions in line with the requirements of the assessment brief. Where required by the assessment, candidates must also have access to AI-enabled analytical tools. Centres are responsible for ensuring that all hardware, software and assessment resources required to complete the assessment are available throughout the supervised assessment period.

Content

5.1 User requirements, analysis and solution planning

This topic introduces the principles of analysing user requirements and planning digital solutions to meet defined organisational and user needs. Learners develop knowledge and understanding of how user requirements are identified, interpreted and translated into solution designs, alongside the role of problem analysis, success criteria and feasibility assessment in supporting effective decision making. The topic emphasises the importance of considering constraints, governance requirements and collaborative decision making when planning digital solutions, ensuring that proposed approaches are practical, secure, accessible and fit for purpose.

In this topic learners will gain knowledge, understanding and skills in the following areas:
5.1.1 User needs and requirements
5.1.2 Problem definition and analysis
5.1.3 Requirements, success criteria and feasibility
5.1.4 Constraints, governance and decision making

Section	Amplification
5.1.1 User needs and requirements	Learners should know and understand: • the purpose of analysing user needs and requirements when designing digital solutions • the relationship between user needs, workplace context and effective digital solution design • how workplace requirements and user needs inform configuration decisions, and how these decisions influence system functionality, performance, usability, accessibility and security • how user needs are identified, interpreted and translated into digital solution designs, including the role of feedback, iteration and shared understanding in refining solutions. Learners should be able to interpret defined user needs and requirements to inform solution design.

DRAFT

© WJEC CBAC Ltd 2027.

5.1.2 Problem definition and analysis	Learners should know and understand:
	• approaches used to define problems, determine solution scope and identify constraints, including:
	  • identifying user needs and requirements
	  • distinguishing between essential and desirable features
	  • identifying assumptions and dependencies
	  • recognising technical, organisational and resource constraints
	  • distinguishing between stated requirements and underlying user needs
	  • considering the availability, quality and suitability of data required to support solution objectives
	• the role of analysis and planning in reducing risk during later stages of development, such as:
	  • identifying risks early
	  • evaluating alternative approaches
	  • reducing rework
	  • improving development efficiency.
	
	Learners should be able to:
	• analyse a problem to identify:
	  • inputs
	  • outputs
	  • constraints
	  • assumptions
	  • success criteria.

5.1.3 Requirements, success criteria and feasibility	Learners should know and understand:
	• the role of requirements, assumptions and success criteria in shaping solution proposals, including:
	  • validation of assumptions relating to data quality, completeness, availability and feasibility
	  • consideration of how assumptions influence solution effectiveness
	  • establishing measurable success criteria.
	  • how defined requirements and test outcomes are used to evaluate system readiness for deployment and continued use, including the application of performance thresholds and consideration of trade-offs between performance, usability and security.

5.1.4 Constraints, governance and decision making	Learners should know and understand:
	• the influence of technical, organisational and resource constraints on solution feasibility and implementation, including:
	  • data protection and the appropriate use of personal and sensitive information
	  • data availability, quality
	  • security requirements, including authentication and access control
	  • accessibility requirements and the needs of diverse users
	  • acceptable use of systems, devices and services
	  • available budgets
	  • staff expertise
	  • existing infrastructure
	  • timescales
	  • workplace policies and procedures

© WJEC CBAC Ltd 2027.

	• how technical, organisational and resource constraints influence collaborative decision making and digital solution design, and the importance of inclusive and responsible collaboration in achieving effective outcomes.
	
	Learners should be able to:
	• identify and document technical, organisational and resource constraints that may affect proposed solutions clearly and accurately, including:
	  • constraints relating to technology, infrastructure, budgets, expertise and timescales
	  • identifying factors that may affect solution feasibility or implementation
	  • recording constraints, assumptions and dependencies using appropriate documentation
	• justify design decisions in relation to user needs and requirements and governance considerations, including:
	  • explaining how proposed solutions address identified user needs and requirements
	  • considering usability, accessibility and security requirements
	  • considering governance requirements relating to data protection, responsible design and automated or AI-enabled systems
	  • explaining how constraints, assumptions and requirements have influenced design decisions.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.2.1 Configuration requirements
- 1.2.2 Configuration dependencies and consistency
- 1.2.3 Configuration for workplace and user requirements
- 1.3.1 Requirements and the purpose of testing
- 1.3.2 Test outcomes and evidence
- 1.3.3 Performance thresholds and system quality
- 1.3.4 Performance, usability and security trade-offs
- 1.3.5 Judging system readiness
- 1.6.2 Identifying and interpreting user needs
- 1.6.3 Translating needs into digital solution requirements
- 1.6.4 Constraints and inclusive decision making

DRAFT

© WJEC CBAC Ltd 2027.

5.2 Analyse, design and communicate digital solutions

This topic introduces the principles of analysing, designing and communicating digital solutions to address defined user and organisational needs. Learners develop knowledge and understanding of structured problem solving, computational thinking, algorithms and solution logic, alongside the role of digital systems, data requirements and feasibility considerations in shaping solution designs. The topic emphasises the use of logical and structured approaches to develop effective solution proposals and the communication of design ideas through a range of technical representations and documentation formats.

In this topic learners will gain knowledge, understanding and skills in the following areas:
5.2.1 Structured logic and problem solving
5.2.2 Algorithms and computational thinking
5.2.3 Digital systems and solution feasibility
5.2.4 Design representation and communication

Section	Amplification

5.2.1 Structured logic and problem solving	Learners should know and understand:
	• the role of structured logic and step-by-step processes in designing digital solutions, including:
	  • inputs
	  • processes
	  • outputs
	• the relationship between logical structure and predictability of outcomes
	• the contribution of structured problem-solving and logical thinking to robust solution proposals.
	
	Learners should be able to structure a proposed digital solution using logical steps and processes.

5.2.2 Algorithms and computational thinking	Learners should know and understand:
	• principles of algorithms and structured coding approaches used to represent, sequence and control solution logic within digital designs
	• principles, concepts and approaches underpinning digital design and structured logic in low-code and block-based environments, including:
	  • abstraction
	  • decomposition
	  • sequencing
	  • selection
	• iteration how these principles support the development of reliable and maintainable digital solutions
	• how these principles and structured approaches are used to develop, test and refine digital solutions.
	
	Learners should be able to:
	• apply abstraction and decomposition to break complex problems into manageable components, such as:
	  • identifying relevant and irrelevant information
	  • breaking problems into smaller tasks or components
	  • focusing on key requirements and functionality
	  • organising components to support solution development.

DRAFT

© WJEC CBAC Ltd 2027.

5.2.3
Digital systems and solution feasibility
	Learners should know and understand:
	• how digital systems, components and processes and data requirements can influence solution feasibility and the structure of proposed solutions, including trade-offs between:
	  • functionality
	  • complexity
	  • maintainability
	  • data quality and availability requirements
	  • how the main components of digital systems, including hardware, software, network infrastructure, data storage and user interfaces, and the relationship between these components within overall system structures.

5.2.4
Design representation and communication
	Learners should be able to:
	• represent solution ideas using specified technical design techniques and formats, such as:
	  • flowcharts and process diagrams
	  • wireframes, storyboards and mock-ups
	  • system diagrams and data flow representations
	  • pseudocode and structured logic representations
	  • requirements documentation and design specifications
	  • presentations, reports, spreadsheets and other technical documentation formats.

Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.1.1 Digital systems and their components • 1.7.1 Structured problem solving • 1.7.2 Algorithms, solution logic and control structures • 1.7.3 Designing structured digital solutions • 1.7.4 Developing, testing and refining solutions	

DRAFT

© WJEC CBAC Ltd 2027.

5.3 Prototyping and development approaches

This topic introduces the principles and approaches used to develop, prototype and refine digital solutions to meet defined user and organisational requirements. Learners develop knowledge and understanding of structured development approaches, prototyping techniques and the use of low-code, block-based and AI-supported tools to create and evaluate solution ideas. The topic emphasises the importance of iterative development, critical evaluation of AI-generated outputs, and the consideration of ethical, legal and governance requirements when designing, refining and justifying digital solutions.

In this topic learners will gain knowledge, understanding and skills in the following areas:
5.3.1 Development approaches and prototyping
5.3.2 AI-supported solution development
5.3.3 Prototyping and development approaches
5.3.4 Solution evaluation and design justification

Section	Amplification

5.3.1 Development approaches and prototyping	Learners should know and understand:
	• how structured development approaches apply computational thinking principles to support prototyping, testing and refinement of solution ideas
	• the purpose and characteristics of low-code and block-based development approaches, including how they support:
	  • rapid prototyping
	  • iterative development
	  • early-stage exploration of digital solution ideas
	• the purpose of prototypes in demonstrating, testing and refining solutions functionality prior to implementation.
	
	Learners should be able to:
	• create a prototype of a digital solution that demonstrates core features, user interaction and intended functionality, and use feedback and evaluation to refine the prototype
	• develop and refine solution concepts using low-code, block-based or AI-supported approaches.

5.3.2 AI-supported solution development	Learners should know and understand:
	• the role of AI-enabled systems in supporting solution design, including:
	  • generating solution ideas
	  • refining approaches
	  • evaluating potential solutions
	• the importance of assessing the suitability, reliability and limitations of AI-generated outputs
	• how prompts and structured inputs are used to generate outputs from automated and AI-enabled systems, including how prompt design influences:
	  • output quality
	  • the relevance and accuracy of generated outputs
	  • limitations of automated generated outputs
	  • broader social and ethical implications of automated and AI-enabled systems and their outputs.

DRAFT

© WJEC CBAC Ltd 2027.

	Learners should be able to:
	• use appropriate development tools, environments and structured inputs, including prompts, to create, refine or represent digital solutions, such as:
	  • low-code and block-based development environments
	  • prototyping and design tools
	  • wireframing and mock-up tools
	  • flowcharting and process modelling tools
	  • collaborative design and planning tools
	  • automated and AI-enabled systems used to generate, refine or evaluate solution ideas
	  • prompts and structured inputs used to generate outputs from automated and AI-enabled systems
	  • templates and frameworks used to support consistent solution design and documentation.

5.3.3 Prototyping and development approaches	Learners should know and understand:
	• the implications of incorporating automated and AI-enabled processes into digital solutions, such as:
	  • efficiency and productivity benefits
	  • accuracy and reliability of outputs
	  • bias and limitations
	  • human oversight and accountability
	  • impacts on users and organisations
	• potential risks associated with automated decision-making and their implications for users and organisations, including:
	  • bias
	  • inaccurate outputs
	  • inappropriate reliance on automated systems
	  • lack of transparency
	  • limitations of automated decision-making
	  • the need for human oversight
	• how ethical, legal and sustainability considerations relevant to digital practice, including:
	  • intellectual property rights
	  • ownership
	  • attribution
	  • responsible use of automated and AI-enabled systems and their outputs.
	
	Learners should be able to explain how the limitations and potential bias of AI-enabled systems can influence decision-making outcomes, and the importance of human oversight in supporting responsible use.

5.3.4 Solution evaluation and design justification	Learners should be able to:
	• justify design decisions in relation to user needs and requirements and governance considerations, including:
	  • meeting identified user and organisational requirements
	  • usability, accessibility and security considerations
	  • data protection and responsible design requirements
	  • governance requirements for automated and AI-enabled systems
	  • the impact of constraints, assumptions and dependencies on design decisions.

© WJEC CBAC Ltd 2027.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.8.1 Artificial intelligence fundamentals
- 1.8.3 AI capabilities, limitations and decision making
- 1.8.4 Prompts, structured inputs and generated outputs
- 1.8.5 Ethical, legal, social and sustainable digital practice

DRAFT

© WJEC CBAC Ltd 2027.

5.4 User-centred, secure and responsible digital solution design

This topic introduces the principles of designing digital solutions that are user-centred, secure, accessible and responsible. Learners develop knowledge and understanding of user experience, interface design, accessibility, data protection and security, alongside the governance requirements that support ethical and effective digital practice. The topic emphasises the importance of meeting diverse user needs, safeguarding personal and sensitive information, applying responsible approaches to the use of automated and AI-enabled systems, and communicating digital solutions in ways that promote usability, sustainability and positive user outcomes.

In this topic learners will gain knowledge, understanding and skills in the following areas:

5.4.1 User experience and interface design
5.4.2 Accessibility and inclusive design
5.4.3 Data protection, security and access control
5.4.4 Responsible design, governance and AI-enabled systems
5.4.5 Communication and sustainability

Section	Amplification

5.4.1 User experience and interface design	Learners should know and understand:
	• principles of user experience and user interface design that support usability and accessibility
	• the relationship between interface design and user behaviour
	• how design decisions influence digital solutions, such as:
	  • usability
	  • accessibility
	  • user interaction
	  • system behaviour.
	
	Learners should be able to:
	• design solution concepts that consider:
	  • system behaviour
	  • user interaction
	  • accessibility requirements.

5.4.2 Accessibility and inclusive design	Learners should know and understand:
	• policies and procedures and their influence on solution proposals relating to:
	  • accessibility
	  • data protection
	  • security
	  • responsible design
	• designing for accessibility and diverse user needs, such as:
	  • accessibility of content and functionality
	  • adaptable presentation and access methods
	  • clear and consistent navigation
	  • compatibility with assistive technologies
	  • inclusive user testing
	  • intuitive interaction and interface design.
	
	Learners should be able to evaluate design proposals against accessibility and governance requirements.

DRAFT

© WJEC CBAC Ltd 2027.

5.4.3
Data protection, security and access control
	Learners should know and understand:
	• protection and appropriate use of personal and sensitive information, including:
	  • privacy and confidentiality requirements
	  • collection and use of information for appropriate purposes
	  • ensuring data is accurate, relevant and suitable for its intended purpose
	  • secure storage and handling of data
	  • compliance with organisational policies and legal requirements relating to data protection
	• secure authentication and access control, such as:
	  • management of user identities and accounts
	  • permissions and access rights
	  • authorised access and restrictions.

5.4.4
Responsible design, governance and AI-enabled systems
	Learners should know and understand:
	• responsible and ethical use of automated and AI-enabled systems, such as:
	  • bias and limitations in automated outputs
	  • transparency of automated processes and decisions
	  • accountability for decisions and outcomes
	  • appropriate human oversight and intervention
	  • verification of automated and AI-generated outputs
	• governance requirements relevant to digital solutions that use automated and AI-enabled components, such as:
	  • organisational policies and procedures
	  • accountability and responsibility for decisions
	  • transparency and explainability of automated processes
	  • monitoring and review of automated systems
	  • compliance with legal, ethical and regulatory requirements
	• the importance of oversight, accountability and transparency in digital solution design.
	
	Learners should be able to:
	• justify design decisions in relation to user needs, ethical considerations and organisational requirements, including:
	  • user requirements
	  • accessibility and usability considerations
	  • security and data protection requirements
	  • organisational constraints.

5.4.5
Communication and sustainability
	Learners should know and understand:
	• how communication approaches influence clarity, efficiency and user experience, including:
	  • adapting communication to meet diverse audience needs
	  • use of appropriate language and terminology
	  • selection of appropriate communication methods
	  • distinguishing between user support and technical troubleshooting activities
	• how professional, ethical and responsible communication supports the effective handling of technical information, including maintaining accuracy and consistency, adapting language to audience needs through appropriate technical and non-technical language, protecting

DRAFT

© WJEC CBAC Ltd 2027.

	confidentiality and privacy, and responding appropriately to user queries and expectations
	• sustainability considerations in digital solution design, including:
	  • efficient use of processing resources
	  • efficient use of storage resources
	  • energy consumption
	  • device lifecycle considerations
	  • reducing unnecessary resource utilisation.
	
	Learners should be able to:
	• communicate proposed solutions clearly to technical and non-technical audiences
	• consider system behaviour, user interaction, accessibility and responsible design principles when creating design solution concepts, such as:
	  • navigation, usability and user experience
	  • privacy, security and data protection requirements
	  • responsible and ethical use of automated and AI-enabled systems
	  • sustainability and efficient use of digital resources.

Synoptic links to Foundations of Digital Systems and Data This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including: • 1.5.1 Communication in technical support • 1.5.2 Adapting communication for users • 1.5.3 Professional, ethical and responsible communication	

DRAFT

© WJEC CBAC Ltd 2027.

5.5 Analyse, design and communicate digital solutions

This topic introduces the principles of analysing, designing and communicating digital solutions to meet user and organisational requirements. Learners develop knowledge and understanding of how solution ideas are represented and documented, the role of collaboration and stakeholder feedback in refining designs, and the importance of communicating technical information effectively to different audiences. The topic emphasises the evaluation and justification of design decisions, ensuring that digital solutions are accessible, responsible, sustainable and aligned with user needs, governance requirements and organisational constraints.

In this topic learners will gain knowledge, understanding and skills in the following areas:

5.5.1 Design representation and solution proposals
5.5.2 Collaboration, user feedback and solution refinement
5.5.3 Communication of technical information and solutions
5.5.4 User experience, accessibility and responsible design

Section	Amplification

5.5.1 Design representation and solution proposals	Learners should know and understand:
	• the purpose of low-fidelity representations in communicating solution ideas during early stages of design
	• the role of documentation and shared understanding in enabling development decisions.
	
	Learners should be able to:
	• produce a clear and structured solution proposal suitable for development
	• represent solution ideas using specified technical formats, such as:
	  • documents
	  • presentations
	  • spreadsheets
	  • databases
	  • diagrams
	  • document assumptions, decisions and constraints clearly and accurately.

5.5.2 Collaboration, user feedback and solution refinement	Learners should know and understand: • how collaboration supports digital solution development, including the role and responsibilities of stakeholders, the value of differing perspectives and expertise, and the use of structured approaches to support shared decision making, problem solving and solution quality • how user needs and feedback inform digital solution design, and how iteration, shared understanding and solution refinement contribute to the development of effective solutions that meet user and organisational requirements Learners should be able to: • obtain and review feedback from stakeholders • evaluate how effectively a digital solution meets identified requirements • make reasoned recommendations for refinement and improvement.

DRAFT

© WJEC CBAC Ltd 2027.

5.5.3 Communication of technical information and solutions	Learners should know and understand:
	• the importance of communicating technical information and proposed solutions clearly to both technical and non-technical audiences
	• how communication approaches influence clarity, efficiency and user experience, including the need to adapt communication to meet diverse user needs and to distinguish between communication-based support and technical troubleshooting requirements
	• how communication approaches influence the clarity, accuracy and effectiveness of technical information, including the use of appropriate technical and non-technical language, maintaining confidentiality and privacy, adapting communication to audience needs, and responding appropriately to user queries and expectations.
	
	Learners should be able to:
	• communicate proposed solutions clearly to:
	  • technical audiences
	  • non-technical audiences.

5.5.4 User experience, accessibility and responsible design	Learners should be able to:
	• justify design decisions in relation to:
	  • user requirements
	  • governance requirements
	  • organisational constraints
	  • data quality, availability and suitability requirements
	  • ethical and sustainability considerations
	• justify how defined requirements, performance thresholds, test outcomes inform decisions about system readiness for deployment and continued use, including:
	  • evaluation of functionality
	  • comparison of test outcomes against requirements and success criteria
	  • performance and reliability
	  • consideration of trade-offs between performance, usability and security.

Synoptic links to Foundations of Digital Systems and Data
This section is underpinned by knowledge and understanding from relevant areas of the Foundations of Digital Systems and Data content, including:

- 1.3.1 Requirements and the purpose of testing
- 1.3.2 Test outcomes and evidence
- 1.3.3 Performance thresholds and system quality
- 1.3.4 Performance, usability and security trade-offs
- 1.3.5 Judging system readiness
- 1.5.1 Communication in technical support
- 1.5.2 Adapting communication for users
- 1.5.3 Professional, ethical and responsible communication
- 1.6.1 Collaboration in digital work
- 1.6.3 Translating needs into digital solution requirements
- 1.6.4 Constraints and inclusive decision making

© WJEC CBAC Ltd 2027.

Transferrable skills

	Planning when identifying steps, sequencing activities and considering constraints when designing a digital solution	Analysing when examining user needs, system requirements and constraints to structure solutions	Communicating when explaining solution proposals and explaining design decisions clearly to technical and non-technical audiences
5.1.1	✓	✓	
5.1.2	✓	✓	
5.1.3			
5.1.4	✓	✓	✓
5.2.1	✓	✓	
5.2.2	✓	✓	
5.2.3		✓	
5.2.4			✓
5.3.1	✓		
5.3.2	✓	✓	
5.3.3		✓	
5.3.4		✓	✓
5.4.1			
5.4.2		✓	✓
5.4.3			✓
5.4.4		✓	✓
5.4.5		✓	✓
5.5.1	✓		✓
5.5.2		✓	✓
5.5.3	✓		✓
5.5.4		✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

Work-related behaviours				
	Inclusive in considering diverse user needs, accessibility requirements and fair representation in data and digital solutions	Creative when developing and proposing digital solutions to meet defined user needs and constraints	Adaptable when responding to changing requirements, system behaviour or feedback during problem solving and solution development	Self-aware in recognising limitations, reflecting on decisions and seeking support or clarification when appropriate
5.1.1	✓	✓		
5.1.2	✓	✓	✓	
5.1.3		✓		
5.1.4		✓	✓	
5.2.1		✓		
5.2.2		✓		
5.2.3		✓		
5.2.4				
5.3.1		✓	✓	
5.3.2		✓	✓	✓
5.3.3	✓			✓
5.3.4	✓		✓	✓
5.4.1				
5.4.2	✓		✓	✓
5.4.3	✓			
5.4.4	✓		✓	✓
5.4.5	✓		✓	✓
5.5.1				✓
5.5.2	✓		✓	✓
5.5.3	✓			
5.5.4	✓		✓	✓

DRAFT

© WJEC CBAC Ltd 2027.

3. Assessment

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

3.1. Assessment objectives and weightings

Below are the assessment objectives for this qualification. Learners must:

AO1
Demonstrate knowledge and understanding of concepts, principles, requirements and approaches relevant to the subject area.

AO2
Apply knowledge and understanding of concepts, principles, requirements and approaches to plan, carry out tasks, produce outputs, and use information appropriately.

AO3
Analyse and evaluate information, situations and evidence to make judgements, draw conclusions and make recommendations.

The table below shows the weighting of each assessment objective for each assessment and for the qualification as a whole.

	AO1	AO2	AO3	Total
Assessment 1	10	6	4	20
Assessment 2	5	9	6	20
Assessment 3	3	10	7	20
Assessment 4	3	10	7	20
Assessment 5a/b	4	10	6	20
Overall weighting	25	45	30	100

3.2. Assessment overview

Assessment 1

Content Area 1 – Assessment 1 is assessed through an externally set and marked on-screen-only 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).

© WJEC CBAC Ltd 2027.

This assessment is subject to the qualification's terminal assessment requirement. Learners must take the assessment at the end of their programme of study, having completed all, or substantially all, of the qualification content.

This assessment is externally set and marked by WJEC.

Assessment 2

Content Area 1 – Assessment 2 is assessed through an externally set and marked on-screen-only case study 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 subject to the qualification's terminal assessment requirement. Learners must take the assessment at the end of their programme of study, having completed all, or substantially all, of the qualification content.

This assessment is externally set and marked by WJEC.

Assessment 3

Content Area 2 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 from the last week in February for use within that academic year. Learners must not have access to the brief or associated tasks until the start of the assessment.

Learners are provided with the assessment window in which to complete the assessment. This flexibility allows centres to integrate the assessment within their programme of delivery while providing sufficient opportunity for learners to engage with the tasks, produce evidence, and demonstrate the knowledge, skills and understanding required by the content area under controlled conditions.

Assessment sessions may be arranged across multiple sittings within the 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.

Assessment 4

Content Area 3 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 from the last week in February for use within that academic year. Learners must not have access to the brief or associated tasks until the start of the assessment.

Learners are provided with the assessment window in which to complete the assessment. This flexibility allows centres to integrate the assessment within their programme of delivery while providing sufficient opportunity for learners to engage with the tasks, produce evidence, and demonstrate the knowledge, skills and understanding required by the content area under controlled conditions.

© WJEC CBAC Ltd 2027.

DRAFT

Assessment sessions may be arranged across multiple sittings within the 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.

Assessment 5a (Optional)

Content Area 4 is assessed through an externally set non-exam assessment, which is set and marked 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 from the last week in February for use within that academic year. Learners must not have access to the brief or associated tasks until the start of the assessment.

Learners are provided with the assessment window in which to complete the assessment. This flexibility allows centres to integrate the assessment within their programme of delivery while providing sufficient opportunity for learners to engage with the tasks, produce evidence, and demonstrate the knowledge, skills and understanding required by the content area under controlled conditions.

Assessment sessions may be arranged across multiple sittings within the 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.

Assessment 5b (Optional)

Content Area 5 is assessed through an externally set non-exam assessment, which is set and marked 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 from the last week in February for use within that academic year. Learners must not have access to the brief or associated tasks until the start of the assessment.

Learners are provided with the assessment window in which to complete the assessment. This flexibility allows centres to integrate the assessment within their programme of delivery while providing sufficient opportunity for learners to engage with the tasks, produce evidence, and demonstrate the knowledge, skills and understanding required by the content area under controlled conditions.

Assessment sessions may be arranged across multiple sittings within the 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.

DRAFT

© WJEC CBAC Ltd 2027.

4. Technical information

4.1. Assessment availability

Assessment	Summer Yr-1	Summer Yr-2
Fundamentals of Digital Systems and Data Assessment 1	×	✓
Foundations of Digital Systems and Data Assessment 2	×	✓
Data Analysis and Insights Assessment 3	✓	✓
Cyber Security and Secure Digital Systems Assessment 4	✓	✓
Digital Solution Design and Development Assessment 5a	×	✓
Digital Solution Design and Development Assessment 5b	×	✓

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
Assessment 1	
Assessment 2	
Assessment 3	
Assessment 4	
Assessment 5a	
Assessment 5b	

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

© WJEC CBAC Ltd 2027.

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. Grading and reporting

Assessments within WJEC V Levels are awarded on a seven-point scale A* to E and P (pass).

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

	Max.	**A***	**A**	**B**	**C**	**D**	**E**	**P**
Assessment 1	120	108	96	84	72	60	48	36
Assessment 2	120	108	96	84	72	60	48	36
Assessment 3	120	108	96	84	72	60	48	36
Assessment 4	120	108	96	84	72	60	48	36
Assessment 5a	120	108	96	84	72	60	48	36
Assessment 5b	120	108	96	84	72	60	48	36

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

V Level qualifications are reported on a seven-point scale: A* to E, P (pass) and U (unclassified).

	Max.	**A***	**A**	**B**	**C**	**D**	**E**	**P**
Qualification	600	540	480	420	360	300	240	180

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

© 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.
Accessible	Designed so that people with a wide range of abilities, needs and characteristics can use a system, product or service effectively.
Accessibility	The extent to which a digital system, product or service can be used by people with a wide range of abilities, needs and characteristics.
Algorithm	A defined sequence of instructions that a computer follows to process inputs and produce an output or solve a problem.
Analytical technique	A structured method used to examine data in order to identify patterns, relationships, comparisons or trends that support conclusions or decision making.
Anomaly	A result, event or pattern that differs significantly from what is expected or from normal behaviour.
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.
Assurance	Activities undertaken to confirm that systems, processes or outputs meet defined requirements, standards or quality expectations.
Authentication	The process of verifying the identity of a user, device or system before allowing access to a system, service or data.
Automated output	Information or results produced automatically by digital tools or systems using defined rules, algorithms or data- driven processes.
Brief	A statement that defines a task, including its purpose, requirements, constraints and intended outcome.
Component	A hardware or software element that forms part of a larger digital system or product and contributes to its operation.
Compliance	Conformity with defined workplace policies, procedures, regulatory requirements or standards.
Configuration	The process of setting or adjusting parameters in hardware or software so that a system operates correctly and securely for its intended purpose.

DRAFT

© WJEC CBAC Ltd 2027.

Control (security control)	A measure, safeguard or procedure designed to reduce risks to systems, services or data.
Controlled environment	A physical or virtual environment used to configure, test or modify systems without affecting live operational systems or users.
Data	Recorded information that can be stored, processed, analysed or transmitted by digital systems.
Data validation	Checks carried out to ensure that data is complete, correctly formatted and within expected ranges before it is used.
Dataset	A structured collection of related data items organised so that they can be stored, processed, analysed or presented.
Dependency	A relationship in which one component, process or service relies on another in order to function correctly.
Device	A piece of hardware that performs a computing function or connects to a digital system.
Digital solution	A proposed or implemented way of addressing a need or solving a problem using digital technologies.
Digital system	A set of connected components, including hardware, software, data and users, which work together to deliver a digital function or service.
Documentation conventions	Agreed formats or structures used to record technical information clearly and consistently.
Escalation	The process of referring an issue, fault or concern to a higher level of responsibility in line with defined procedures.
Field definition	Information that describes the name, data type and purpose of a field or column within a dataset.
Human oversight	The involvement of people in reviewing, validating and making decisions about outputs or actions generated by automated or AI-enabled systems.
Indicator	A measurable sign or observable pattern that provides evidence about system behaviour, performance or potential risk.
Insight	A meaningful interpretation or conclusion derived from analysing information or data.
Interface	A point of interaction where users, devices or systems exchange information.
Interpret	To determine the meaning or implications of information in relation to a defined purpose or question.

DRAFT

© WJEC CBAC Ltd 2027.

Lifecyle practices	Activities associated with the deployment, maintenance, updating and decommissioning of digital systems or devices.
Log	A recorded account of events or activity generated by a digital system.
Low-code tool	A development environment that enables digital solutions to be created using graphical interfaces with minimal manual coding.
Machine learning	A subset of artificial intelligence in which models learn patterns from data to make predictions, classifications or decisions.
Metadata	Information that describes the structure, origin, format or meaning of data.
Monitoring dashboard	A digital interface that displays system activity, alerts or performance information.
Multi-factor authentication (MFA)	An authentication method requiring two or more different factors to verify identity.
Outcome	The result produced by an action, process or system.
Outlier	A data value that differs significantly from other values within a dataset.
Performance	The effectiveness, speed or reliability with which a system operates.
Programming	The process of designing, writing, testing and refining code to create a digital solution that meets a defined purpose.
Protocol	A defined set of rules that governs how data is transmitted and received between devices or systems.
Principle of least privilege	Users, devices, applications and systems should only be given the minimum level of access they need to perform their role or task, and no more.
Quality assurance	Activities and procedures used to confirm that systems, processes or outputs meet defined requirements, standards or quality expectations.
Recommendation	A proposed course of action that is supported by analysis, evidence or evaluation.
Requirement	A stated condition or capability that a system or solution must satisfy.
Risk	The possibility that an event or action may cause harm, loss or disruption to systems, data or services.
Service	A digital function or capability made available to users.
Structured approach	A systematic and organised method for completing a task using defined stages or procedures.

DRAFT

© WJEC CBAC Ltd 2027.

System log	A recorded account of system events, errors or access activity used to monitor system behaviour.
Test	An activity carried out to check whether a system, program or component behaves as expected.
Threat actor	An individual, group or organisation that may intentionally cause harm to systems, services or data.
Usability	The ease with which intended users can understand and operate a system or product.
User interface	The visual and interactive elements through which a user interacts with a digital system, application or device.
User need	A requirement or problem that a digital system or product is designed to address.
User requirement	A statement describing what a user needs a system or product to do in order to achieve a particular task or outcome.
Validation	The process of confirming that data or a system meets defined rules, requirements or conditions.
Version control	A process for managing changes to files, documents or digital assets by tracking revisions and maintaining records of updates.
Vulnerability	A weakness in a system, configuration, process or control that could be exploited to compromise security, functionality or reliability.

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.
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	• 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.
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

DRAFT

© WJEC CBAC Ltd 2027.

	• submit an incident report using a restricted or simulated secure reporting route. Any of these can be used for teaching and learning, however the CA3 assessment 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.

DRAFT

© WJEC CBAC Ltd 2027.

Appendix C – Links to Occupational Standards

The subject content for this V Level draws upon the following Occupational Standards.

Occupational Standard	Reference	SOC Code
Cyber Security Technician	ST0865	2139
Data Technician	ST0795	3132
Digital Device Repair Technician	ST0682	5245
Digital Support Technician	ST0120	3131
Information Communications Technician	ST0973	3131
IT Solutions Technician	ST0505	2137/2139
Software Development Technician	ST0128	2136

DRAFT

© WJEC CBAC Ltd 2027.

Appendix D – Links to Digital Systems and Data Foundation Certificate

The following aspects of content directly relate to content specified in the Digital Systems and Data Foundation Certificate.

V Level Reference	Foundation Certificate Reference	Knowledge and Understanding	Skills
WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making And Core Knowledge and Understanding	LO1: Data handling, analysis and communication	Principles of data handling, data quality, processing and analysis	Preparing, analysing and presenting data to generate insights and support decision making
WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making	LO6: Evidence-based analysis and decision making	Use of data and evidence to support conclusions and judgements	Interpreting findings and making justified, evidence-based decisions
WRP2: Apply security protocols and interpret system information to detect and escalate cyber security concerns And Core Knowledge and Understanding	LO2: Digital systems, configuration and cyber security	Digital systems and cyber security principles, including threats, vulnerabilities and controls	Applying security procedures, interpreting system information and managing system use securely

DRAFT

© WJEC CBAC Ltd 2027.

WRP2: Apply security protocols and interpret system information to detect and escalate cyber security concerns	LO2: Cyber security awareness, risk identification and response	Identification of risks, vulnerabilities and secure system practices	Recognising threats, applying protective actions and escalating concerns in line with procedures
WRP3: Prepare, configure and assure readiness of digital systems to meet user needs (optional) And Core Knowledge and Understanding	LO4: System setup, testing and performance checking	System configuration, testing approaches and performance considerations	Preparing, configuring and testing systems to ensure readiness and performance
WRP4: Design and create a digital solution to meet defined user needs (optional) And Core Knowledge and Understanding	LO3: Programming logic and structured solution design	Programming logic, algorithms and structured approaches to solution design	Planning, designing, creating, testing and refining structured digital solutions to meet defined user needs

DRAFT

© WJEC CBAC Ltd 2027.