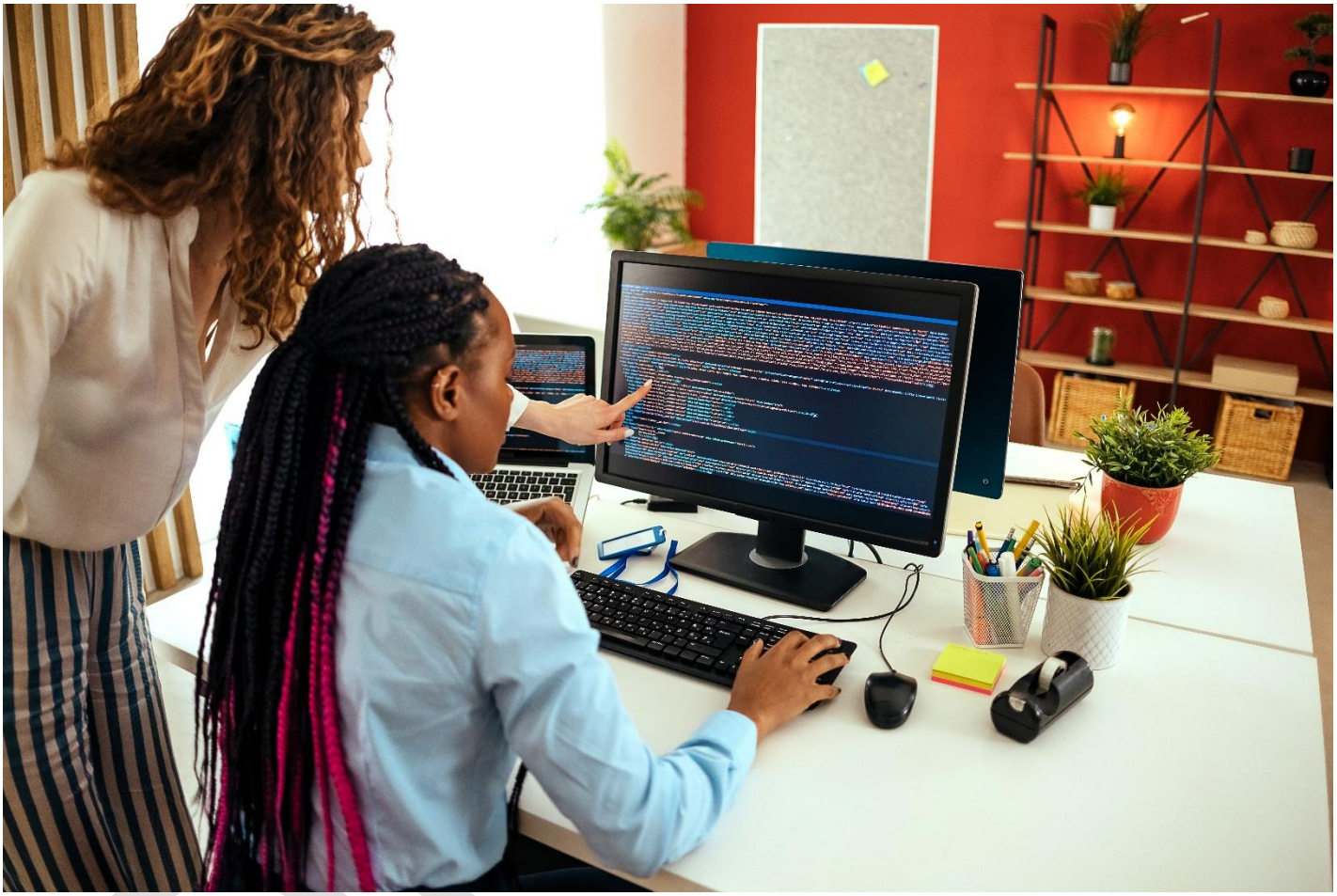
NCFE Level 3 V Level in Digital Systems and Data

QN: TBC

This qualification is currently under regulatory review.
The draft specification is provided for reference only and must not be used for teaching purposes.



Qualification Specification

Qualification summary

Qualification title	**NCFE Level 3 V Level in Digital Systems and Data**
Ofqual qualification number (QN)	TBC
Guided learning hours (GLH)	360
Total qualification time (TQT)	470
Duration	It is expected that this qualification will be delivered over 2 years.
Minimum age	16
Qualification aim	This qualification is designed for 16- to 19-year-olds seeking a broad vocational route in digital systems, data and solution design. It develops learners' knowledge, understanding and skills in applying digital concepts to work with systems and data, manage risks and design solutions, preparing them for progression to further study, higher technical training, or an apprenticeship in a related field.
Grading	This qualification is graded A* to E, P (pass) and U (unclassified).
Assessment method	40% assessment by examination (AbE) 60% non-exam assessment (NEA).
Synoptic assessment	This qualification includes synoptic assessment in both the AbE and NEA, requiring learners to draw together knowledge, understanding and skills from across the full course of study.
Work/industry placement experience	Work/industry placement experience is not required for this qualification.
UCAS	Please refer to the UCAS website for further details of points allocation and the most up-to-date information.
Performance points	Please check the performance points data produced by the Department for Education (DfE).
First award	In line with regulatory requirements, this qualification will not be awarded in the first year it is made available.
Funding	V Levels are funded qualifications. For further guidance on funding, please contact your local funding provider.
Subject content	This qualification has been developed to align with the DfE Digital Systems and Data Level 3 V Level subject content, July 2026.

DRAFT

Contents

Qualification summary **2**

Section 1: introduction **5**

Aims and objectives 5
Guidance for entry and registration 5
Achieving this qualification 6
Progression 6
Progression to higher-level studies 6
Staffing requirements 6
Resource requirements 7
Work/industry placement experience 7
How the qualification is assessed 7
Non-exam assessment (NEA) 8
Assessment by examination (AbE) 8
Moderation 9
Enquiries about results 9
Unclassified grade 9
External assessment conditions 9
Retakes of non-exam assessments (NEAs) 9
Retakes of assessment by examination (AbE) 10
Scheme of assessment 11
Assessment objectives (AOs) 12
Grading information 12
Requirements for referencing 12
Group and collaborative working 13
Plagiarism and use of artificial intelligence (AI) 13
Guidance on delivering sensitive content 13
Access arrangements, reasonable adjustments and paper modifications 14

Section 2: themes and assessment guidance **15**

Delivery guidance 15
Theme 1 Principles of systems, configuration and fault resolution 16
Theme 2 Data analytics and decision-making 21
Theme 3 Principles of communication, problem solving and ethical practice 34
Theme 4 Cyber security operations and response 39
Theme 5 Digital systems configuration and assurance 47
Theme 6 Digital solution design and development 56

Section 3: key terms and definitions **65**

Glossary of terms 65
Digital technology abbreviations 68

Section 4: support **69**

Support materials 69
Other support materials 69
Reproduction of this document 69

Contact us **70**

Appendix A: themes **71**

DRAFT

4

Mandatory themes 71
Optional themes 71

Change history record **72**

DRAFT

Section 1: introduction

Please note this is a draft version of the Qualification Specification and is likely to be subject to change before the final version is produced for the launch of the qualification.

A V Level is a level 3 vocational qualification, aimed at preparing learners for progression to further study, higher technical training, or an apprenticeship.

Centres must ensure they are using the most recent version of the Qualification Specification on the NCFE website.

Aims and objectives

This qualification aims to:

- develop knowledge and understanding of digital systems, data, cyber security and solution design
- develop learners' ability to interpret, analyse and apply digital concepts and skills within a range of work-related contexts to solve problems and support decision-making
- provide a broad level 3 foundation for progression to further study, higher technical training and apprenticeships in related digital disciplines.

The objectives of this qualification are to:

- prepare, analyse, interpret and present data to support decision-making, and apply security protocols to detect and escalate cyber security concerns
- apply core digital knowledge and understanding to either configure and assure digital systems or design and create a digital solution, while developing problem-solving and communication skills, and responsible digital practice.

Guidance for entry and registration

This qualification is designed for 16- to 19-year-olds seeking a broad vocational route into digital systems, data and solution design who want a broad foundation for further study or training.

It is intended to be taken in combination with other qualifications, such as other V Levels, A levels and, where required, level 2 and below English or maths to form a broad study programme.

Registration is at the discretion of the centre in accordance with equality legislation and should be made on the NCFE Portal.

There are no specific prior skills/knowledge a learner must have for this qualification. However, learners may find it helpful if they have already achieved a level 2 qualification in a similar subject area.

Centres are responsible for ensuring that all learners are capable of achieving the knowledge, understanding and skills within all themes of the qualification and complying with the relevant literacy, numeracy, and health and safety requirements.

DRAFT

Achieving this qualification

To be awarded this qualification, learners must complete the required teaching content within mandatory Themes 1 to 4 and either optional Theme 5 or Theme 6, undertake all required assessments and meet the qualification's grading requirements.

Please refer to the list of themes in Appendix A or the theme summaries guidance in Section 2 for further information.

Progression

Learners who achieve this qualification could progress to the following:

- further training or apprenticeships towards careers in digital roles, including:
  - cyber security technician
  - data technician
  - digital device repair technician
  - digital support technician
  - information communications technician
  - IT solutions technician (related roles may be advertised as digital solutions technician)
  - software development technician
- higher education courses in areas such as:
  - computing and information technology
  - data science and data analytics
  - artificial intelligence
  - cyber security
  - digital systems and support
  - digital solution design and software development
  - related digital and technology disciplines.

Progression to higher-level studies

Level 3 qualifications can support progression to higher-level study, which requires knowledge and skills different from those gained at levels 1 and 2. Level 3 qualifications enable learners to:

- apply factual, procedural and theoretical subject knowledge
- use relevant knowledge and methods to address complex, non-routine problems
- interpret and evaluate relevant information and ideas
- understand the nature of the area of study or work
- demonstrate an awareness of different perspectives and approaches
- identify, select and use appropriate cognitive and practical skills
- use appropriate research to inform actions
- review and evaluate the effectiveness of their own methods.

Staffing requirements

Centres delivering any of NCFE's qualifications must:

- have a sufficient number of appropriately qualified/experienced assessors to assess the volume of learners they intend to register

DRAFT

- have a sufficient number of appropriately qualified/experienced internal quality assurers (IQAs) to internally quality assure the anticipated number of assessors and learners
- ensure that all staff involved in assessment and internal quality assurance are provided with appropriate training and undertake meaningful and relevant continuing professional development (CPD)
- implement effective internal quality assurance systems and processes to ensure all assessment decisions are reliable, valid, authentic, sufficient and current – this should include standardisation to ensure consistency of assessment
- provide all staff involved in the assessment process with sufficient time and resources to carry out their roles effectively.

The centre must ensure that individuals undertaking assessor or quality assurer roles within the centre conform to the specified assessment requirements.

Knowledge-based content:

- Assessors will need to be both occupationally knowledgeable and qualified to make assessment decisions.
- IQAs will need to be both occupationally knowledgeable and qualified to make quality assurance decisions.

Competence/skills-based content:

- Assessors will need to be both occupationally competent and qualified to make assessment decisions.
- IQAs will need to be both occupationally knowledgeable and qualified to make quality assurance decisions.

Resource requirements

There are no mandatory resource requirements for this qualification, but centres must ensure learners have access to suitable resources to enable them to cover all the appropriate subject topics.

Work/industry placement experience

Work/industry placement experience is not required for this qualification.

How the qualification is assessed

Assessment is the process of measuring a learner's knowledge, understanding and skills against the standards set in a qualification.

This qualification uses a combination of internal assessment, moderation and external assessment.

Centres must use the NCFE-set assessments as supplied and must not adapt the assessment tasks, contexts or supporting materials.

This qualification is assessed synoptically by both AbE and NEA, allowing learners to:

- demonstrate the ability to draw together different areas of knowledge, understanding and/or skills from across the full course of study

DRAFT

- develop responses that allow them to construct and develop a sustained line of reasoning – or an equivalent logical sequence, depending on the nature of the task – that is coherent, relevant and effectively structured
- demonstrate knowledge, understanding and skills in response to authentic, vocationally related contexts and scenarios.

All learners taking this qualification must be assessed in English and all assessment evidence presented for moderation must be in English.

Non-exam assessment (NEA)

The NEAs within this qualification are externally set, centre marked, with NCFE completing moderation. Centres are not permitted to adapt NEA tasks.

The NEAs will assess the learner's ability to respond to complex and novel situations, drawing on knowledge from specific themes. Learners should not undertake an NEA until the relevant themes have been delivered.

The NEAs encourage learners to combine elements of their learning and demonstrate accumulated knowledge, understanding and skills. This enables learners to show their ability to integrate and apply knowledge, understanding and skills with both breadth and depth.

The NEAs must be supervised and assessed by the tutor. The NEAs will be completed in normal class time within scheduled assessment hours and kept separate from any teaching and learning hours. Information on specific assessment conditions and assessment hours will be available in the NEA brief.

To support delivery, specimen assessment materials for the NEAs are available on the NCFE website.

Where a learner takes this qualification in a single academic year, they complete all assessments within that year using the existing assessment windows. Centres submit marks for all of that learner's NEAs in one submission window. This option is available from the second year the qualification is offered, once all NEAs are available. Please refer to the Assessment Timetable on the NCFE website.

New versions of the NEAs will be produced for each assessment series.

To reduce predictability and maintain assessment integrity, assessment scenarios will vary between series and will be set within a range of realistic contexts.

Assessment by examination (AbE)

The AbE within this qualification is a set date and time (invigilated) examination. NCFE specifies the exact date and time that the external assessment must be administered in the centre. It is administered under specified assessment conditions.

The AbE draws upon the following:

- Theme 1 Principles of systems, configuration and fault resolution
- Theme 2 Data analytics and decision-making
- Theme 3 Principles of communication, problem solving and ethical practice
- Theme 4 Cyber security operations and response.

DRAFT

The AbE material will be sent out by NCFE in time for the start of the assessment. Assessment materials must be kept secure at all times. NCFE marks the AbE. The AbE result contributes to the learner's overall qualification grade.

For further information, centres should refer to the Regulations for the Conduct of External Assessment and Qualification Specific Instructions for Delivery (QSID) documents, available on the NCFE website.

Moderation

Moderation occurs before results are issued and helps us to ensure assessment judgements made by centres are in line with NCFE's guidelines and are reliable across centres. During moderation, the moderator reviews a sample of learners' non-exam assessments (NEAs) and the marks given by assessors within the centre.

Moderators will look at a sample of learners' work. The sample size will be selected using Joint Council for Qualifications (JCQ) sampling guidelines and include assessments from across a range of centre marks, which include a learner with the highest centre mark and a learner with the lowest non-zero centre mark. Where an assessment has been carried out by more than one assessor, all assessors will be included in the sample, where possible.

Enquiries about results

All enquiries relating to learners' results must be submitted in line with our Enquiries about Results and Assessment Decisions Policy, which is available on the NCFE website.

Unclassified grade

A result that does not achieve any grade from A*, A, B, C, D, E or P (pass) will be graded as U (unclassified).

External assessment conditions

To access the external assessment, centres must ensure that learners are booked for the external assessment through the NCFE Portal.

Please refer to the assessment timetable on the NCFE website for specific dates.

For instructions on conducting external assessments, please refer to our Regulations for the Conduct of External Assessment and QSID documents, available on the NCFE website.

Retakes of non-exam assessments (NEAs)

Learners have one retake opportunity for each NEA taken in year one, available in year two. NEA 1 is taken in year one. NEA 2 and NEA 3 are normally taken in year two, but from the second year the qualification is offered, learners may take them in year one and retake them in year two.

The retake could be used to:

- achieve a passing grade
- improve an existing passing grade.

DRAFT

The retake would involve the learner completing a new assessment, within the timeframe stipulated in the published assessment schedule on the NCFE website. Retakes are not capped.

Retakes of assessment by examination (AbE)

AbE is available in one assessment series each year.

Learners must sit the AbE in the assessment series for which certification is claimed. The result from that series is used to calculate their overall qualification grade.

If a learner does not achieve their required grade, they may retake the AbE in a future series, following the normal registration process.

DRAFT

Scheme of assessment

The following table summarises this qualification's scheme of assessment, including raw marks and uniform mark scale (UMS) points.

Assessment	Assessment time	Mandatory/ Optional	Terminal (Yes/No)	Delivery mode	Assessment weightings	Raw marks	UMS	Assessment conditions	Marking
AbE	2 hours	Mandatory	Yes	Paper based or on-screen	40%	90	160	Invigilated	Externally marked
NEA 1	15 hours	Mandatory	No	Computer-based completion and digital submission	20%	48	80	Supervised	Centre marked, externally moderated
NEA 2	12 hours	Mandatory	No	Computer-based completion and digital submission	20%	48	80	Supervised	Centre marked, externally moderated
NEA 3	11 hours (Option A, Theme 5) or 15 hours (Option B, Theme 6)	Mandatory	No	Computer-based completion and digital submission	20%	64	80	Supervised	Centre marked, externally moderated
Assessment total	40 or 44 hours				100%	250	400		

DRAFT

Assessment objectives (AOs)

The assessments for this qualification are mapped against the assessment objectives (AOs) below. These AOs provide a consistent framework for assessing learners' knowledge, understanding and skills. The AOs and their weighting ranges must be met through both timetabled and non-exam assessments.

The weighting of AOs across the qualification will fall within the ranges in the table below, with the total weighting equalling 100%.

The AOs that will be assessed against the content in this qualification are:

AOs		Weighting (%)
AO1	Demonstrate knowledge and understanding of concepts, principles, requirements and approaches relevant to the subject area.	25% to 30%
AO2	Apply knowledge and understanding of concepts, principles, requirements and approaches and to plan, carry out tasks, produce outputs, and use information appropriately.	40% to 45%
AO3	Analyse and evaluate information, situations and evidence to make judgements, draw conclusions and make recommendations.	25% to 30%
Overall weighting of assessment objectives		100%

Grading information

Assessment of this qualification is graded on a seven-point scale: A*, A, B, C, D, E and P (pass), where A* is the highest grade. Learners who do not achieve grade P will receive a U (unclassified) result.

Uniform mark scale (UMS) points for each assessment and grade boundary are set at fixed percentages. When all assessments are completed, the applicable UMS points are combined to determine the overall qualification grade. The AbE result from the assessment series for which certification is claimed must be used.

This qualification uses a 400 UMS framework to ensure consistent, transparent and detailed performance measurement across all assessments.

High performance in one assessment can compensate for lower performance in another. For instance, a high score in the AbE can offset lower scores in the NEAs.

Where a learner retakes an NEA, the higher of the two UMS results will be used.

To accompany results release, NCFE will publish information to support centre understanding of results.

Requirements for referencing

Carefully selected quotations must be included to support learners' own responses within each of the NEAs. Quotations must be made identifiable through the use of quotation marks, bold or italic text and made traceable through referencing at the point of use.

DRAFT

Group and collaborative working

Group and collaborative activities may be used to support the delivery of the qualification content and provide opportunities for learners to develop and apply knowledge, skills and behaviours in a collaborative environment.

For live assessments, centres must follow the instructions provided in the centre guidance and assessment materials, specific to the version of the assessment being delivered. These instructions will define any permitted collaboration, supervision requirements and the nature of evidence that learners are expected to produce.

Plagiarism and use of artificial intelligence (AI)

Work submitted for assessment must be the learner's own work. Using AI to produce work that is then submitted as the learner's own work is malpractice and will have clear consequences under NCFE's malpractice/plagiarism policy.

Centres must have clear AI and malpractice policies in place and communicate these to learners before assessment begins. These policies must outline acceptable and unacceptable uses of AI, define what constitutes malpractice, and explain the consequences of misuse.

Centres must implement appropriate supervision, monitoring and controls over access to digital devices, AI tools and internet connectivity to ensure assessment integrity, maintain the authenticity of learner evidence and help prevent malpractice.

Centres should be alert to indicators of AI use and are required to use suitable plagiarism detection tools as part of their internal quality assurance processes to identify potential misuse of AI and ensure the authenticity of learner evidence.

Detection tools may provide indicators of potential malpractice, but their results should not be relied upon in isolation. Any decision regarding malpractice should be based on a review of all relevant evidence, taking into account the potential for false positive and false negative outcomes.

Any suspected malpractice must be investigated in accordance with the centre's malpractice policy. Centres must report suspected or actual malpractice to NCFE in accordance with NCFE's malpractice and maladministration policy and associated procedures.

Further information can be found on the NCFE website and in JCQ published guidance.

Guidance on delivering sensitive content

When learners engage with sensitive topics, for example cyber incidents, misuse of personal data, online harms or discriminatory automated outputs, centres should:

- recognise the sensitivity of subject content:
  - acknowledge that some topics may evoke strong emotional responses and require careful handling
- equip staff with appropriate training and support:
  - ensure educators are prepared to deliver sensitive content with empathy, awareness, and access to clear support protocols
- foster a safe and supportive learning environment:

    - create spaces where learners feel comfortable discussing sensitive issues, and ensure clear signposting to pastoral care, counselling, or mental health services
- monitor and respond to learners' wellbeing:
    - actively observe learners during and after sessions that cover sensitive content and be ready to offer support or refer learners to appropriate support services where needed.

Access arrangements, reasonable adjustments and paper modifications

These policies are aimed at anyone who uses our products and services and who submits requests for access arrangements, reasonable adjustments or paper modifications. Learners who require access arrangements, reasonable adjustments or paper modifications should discuss their requirements with their tutor.

For more information, please visit the Access arrangements, reasonable adjustments and paper modifications page on the NCFE website.

DRAFT

Section 2: themes and assessment guidance

This section provides details of the structure and content of this qualification, including guided learning hours (GLH), mandatory teaching content and teaching guidance.

Information in the teaching content and mandatory additional information sections must be covered by the tutor during the delivery of the themes. Anything within the teaching guidance is advisory and optional and is intended to provide useful advice and guidance to support delivery of the teaching content.

To make cross-referencing assessment and quality assurance easier, we have used a sequential numbering system in this document for each theme. The numbering system used refers to a theme, subject topic, and teaching content: (for example, 1.1.1 refers to the theme (first number 1), the subject topic within that theme (second number 1.1) and the teaching content within the subject topic (third number 1.1.1)). This will support signposting feedback and tracking.

While studying the qualification, learners should identify and develop a range of individual study skills they can use in order to study effectively.

The glossary in Section 3 must be used in conjunction with the teaching content throughout this Qualification Specification. It provides definitions and clarification of key terms used within the qualification and is intended to support a consistent understanding and interpretation of the content. Centres must refer to the glossary when planning, delivering and assessing the qualification. Section 3 also lists the full terms for abbreviations used in the teaching content.

Delivery guidance

Centres must deliver the teaching content in Themes 1 and 2 before learners undertake NEA 1, which takes place in year one. In addition to Themes 1 and 2, centres must deliver the teaching content in Themes 3 and 4 before learners undertake NEA 2, and the teaching content in the selected optional theme (Theme 5 or Theme 6) before learners undertake NEA 3. NEA 2 and NEA 3 normally take place in year two.

For learners taking the qualification in a single academic year, centres must deliver the content assessed by each NEA before the relevant assessment window.

For further information or guidance about this qualification, please contact our Customer Support team.

DRAFT

Theme 1 Principles of systems, configuration and fault resolution

Theme summary			
The aim of this theme is to provide the conceptual foundation for how digital systems are structured, configured and kept working, covering system components and their roles, configuration decisions and readiness for use, and the causes of faults and the structured approaches used to resolve them.			
Assessment			
Assessment by examination (AbE) and non-exam assessment (NEA)			
Mandatory The teaching content and mandatory additional information must be covered by the tutor during the delivery of this qualification.	**Assessment reference** Refer to the scheme of assessment in Section 1.	**Level 3**	**60 GLH** Refer to the scheme of assessment in Section 1 for AbE and NEA assessment durations.

1.1 Functions of systems, components and architecture

Teaching content The learner must know and understand	Mandatory additional information
1.1.1 The main components of digital systems, and their roles within system structure	• hardware • software • network infrastructure • data storage • user interfaces
1.1.2 The role of operating systems, user accounts and access controls in enabling secure and effective system use	N/A

1.2 Principles of configuration and system readiness

Teaching content The learner must know and understand	Mandatory additional information

1.2.1 Configuration requirements relating to user accounts, access permissions, connectivity, storage and security settings, and the importance of consistency in configuration practices	• dependency relationships between configuration settings and system behaviour
	• methods of managing configuration dependencies:
	  ○ change control
	  ○ documenting configuration state
	  ○ rollback planning
	  ○ testing in non-live environments
	• backup and disaster recovery planning, including business continuity

DRAFT

Teaching content The learner must know and understand	Mandatory additional information
1.2.2 The relationship between workplace requirements, user needs, configuration decisions, and system performance, usability and security	N/A
1.2.3 Configuration-related risks arising from misconfigured access permissions, weak authentication settings, unpatched software, exposed network services and insecure default configurations, and their potential impact on systems and users	N/A

1.2.4 The relationship between defined requirements, test outcomes and decisions about system readiness for deployment and continued use	• defined performance thresholds
	• trade-offs between performance, usability and security
	• factors that inform a deployment readiness decision:
	  ○ user acceptance sign-off
	  ○ rollback capability
	  ○ support readiness
	  ○ timing around business cycles

1.3 Causes of faults and methods of diagnosis and resolution

Teaching content The learner must know and understand	Mandatory additional information

1.3.1 The nature and causes of technical faults in digital systems, and how system behaviour can be interpreted in relation to expected outcomes to support fault identification and resolution	• how faults arise from hardware, software, network and user-related factors
	• causes of faults beyond hardware, software, network and user-related factors:
	  ○ environmental factors
	  ○ third-party service outage
	  ○ configuration drift
	  ○ capacity exhaustion

1.3.2 Structured approaches to diagnosing and resolving faults, and the consequences of inaccurate diagnosis or delayed action	• the role of diagnostic tools, system information and logical processes in supporting accurate identification, decision-making, escalation and restoration of system functionality
	• methods of structured diagnosis:
	  ○ halving
	  ○ elimination
	  ○ reproduce then isolate
	  ○ root cause analysis
	• stages of fault resolution:
	  ○ identification
	  ○ decision-making

DRAFT

Teaching content The learner must know and understand	Mandatory additional information
	○ escalation, including when escalation thresholds are met ○ restoration • types of diagnostic tools and information sources: ○ network diagnostics ○ hardware and software diagnostics ○ ticket history
1.3.3 Principles of safe, secure and responsible practice when diagnosing and resolving faults	• protection of personal and sensitive information • confidentiality and privacy • system integrity and availability • legal and ethical responsibilities • consideration of the impact of actions on users, services and organisations

Teaching guidance
This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive. Some concepts in this theme also appear in the themes that include skills. This theme provides the understanding; those themes are where learners apply it.
1.1 Functions of systems, components and architecture
1.1.1 The main components of digital systems, and their roles within system structure could include: • examples of each component type: ○ processors and memory (hardware) ○ operating systems and applications (software) ○ routers and servers (network infrastructure) ○ local and cloud storage (data storage) ○ graphical and command-line interfaces (user interfaces) • examples of what each component does within a system: ○ hardware, providing the physical processing, storage and connectivity a system depends on ○ software, instructing the hardware and enabling users to carry out tasks ○ network infrastructure, moving data between systems, devices and users ○ data storage, holding data so that it can be retrieved and managed ○ user interfaces, enabling users to interact with and control the system.
1.1.2 The role of operating systems, user accounts and access controls in enabling secure and effective system use No additional teaching guidance is provided for this teaching content.
1.2 Principles of configuration and system readiness
1.2.1 Configuration requirements relating to user accounts, access permissions, connectivity, storage and security settings, and the importance of consistency in configuration practices

DRAFT

Teaching guidance
No additional teaching guidance is provided for this teaching content.

1.2.2 The relationship between workplace requirements, user needs, configuration decisions, and system performance, usability and security could include:
 	
• examples of configuration trade-offs:
  ○ stricter security settings reducing usability, such as more frequent re-authentication
  ○ increased storage or processing allocation, improving performance but increasing cost.

1.2.3 Configuration-related risks arising from misconfigured access permissions, weak authentication settings, unpatched software, exposed network services and insecure default configurations, and their potential impact on systems and users could include:
 	
• examples of how configuration risks arise:
  ○ human error, such as a setting changed without being tested or recorded
  ○ settings left at their default values after installation
  ○ a change applied to one system but not to others that depend on it
• examples of impact on systems and users:
  ○ loss of data or loss of access to a service
  ○ unauthorised access to personal or sensitive information
  ○ disruption to users while the cause is identified and corrected.
 	
Worked example of a misconfigured access permission
A user is mistakenly granted write access to a shared folder when read-only access was intended. The folder contains backup files, which the user deletes while cleaning up their own work. The deletion goes unnoticed until the backups are needed for a restore and are found to be unavailable.

1.2.4 The relationship between defined requirements, test outcomes and decisions about system readiness for deployment and continued use No additional teaching guidance is provided for this teaching content.
1.3 Causes of faults and methods of diagnosis and resolution
1.3.1 The nature and causes of technical faults in digital systems, and how system behaviour can be interpreted in relation to expected outcomes to support fault identification and resolution No additional teaching guidance is provided for this teaching content.
1.3.2 Structured approaches to diagnosing and resolving faults, and the consequences of inaccurate diagnosis or delayed action **Worked example of structured diagnosis and resolution** A computer repeatedly shuts down. The technician investigates potential causes, checking the power supply, cooling system and internal components in turn. The fault is traced to a clogged fan restricting airflow, which causes overheating. The fan is cleaned and the computer is retested to confirm the issue has been resolved. Replacing a component such as the hard drive would have incurred unnecessary cost without addressing the underlying fault. If multiple computers had experienced the same issue, suggesting a wider problem, the fault would have been escalated for further investigation.
1.3.3 Principles of safe, secure and responsible practice when diagnosing and resolving faults

DRAFT

Teaching guidance
No additional teaching guidance is provided for this teaching content.

Transferable skills
No transferable skills have been identified within this theme.

Workplace behaviours
No workplace behaviours have been identified within this theme.

DRAFT

Theme 2 Data analytics and decision-making

Theme summary
The aim of this theme is to develop the knowledge, understanding and skills needed to prepare, analyse, interpret and present data from different sources, so that conclusions are justified and decisions are properly informed.
Assessment
Assessment by examination (AbE) and non-exam assessment (NEA)

Mandatory The teaching content and mandatory additional information must be covered by the tutor during the delivery of this qualification.	**Assessment reference** Refer to the scheme of assessment in Section 1.	**Level 3**	**80 GLH** Refer to the scheme of assessment in Section 1 for AbE and NEA assessment durations.

2.1 Characteristics of data structures, sources and quality

Teaching content The learner must know and understand	**Mandatory additional information**
2.1.1 The purpose of preparing, analysing, interpreting and presenting data to generate insights that support conclusions and decision-making in workplace contexts	N/A
2.1.2 How data is structured, formatted and defined within datasets from different sources	• how levels of detail affect interpretation, comparability and use
2.1.3 Data quality issues arising from missing data, duplicate records, inconsistent formats and conflicting values across sources, and their impact on analysis	N/A
2.1.4 Methods used to validate and prepare data prior to analysis through checking formats and data types, confirming completeness, verifying value ranges and resolving inconsistencies	N/A
2.1.5 The role of metadata, field definitions and documentation in supporting analysis, transparency, accountability and correct interpretation of analysed outputs	N/A

DRAFT

2.2 Methods of preparing and combining datasets

Teaching content The learner must know and understand	Mandatory additional information

2.2.1 How combining datasets from different sources can reveal relationships and insights not visible when sources are analysed separately	• risks associated with inconsistent definitions and alignment across sources
	• effects of combining datasets:
	  ○ covering different time periods or seasonal cycles
	  ○ recorded at different levels of detail
	• causes of duplicate entities across sources
	• effects of differing units, currencies or formats between sources
	• reasons for inconsistent identifiers when matching or joining records
	• effects of missing data or values on combined datasets
	• relationship between invalid and conflicting values for the same record across sources
	• causes of column and field mismatch across sources
	• effects of differing data entry rules between sources

2.2.2 The relationship between data preparation, analytical methods and the reliability of conclusions	N/A

2.2.3 The relationship between data quality, analytical approach, data limitations, uncertainty and confidence in conclusions	• the impact of outliers, sampling bias and unrepresentative data
	• causes of unrepresentative data:
	  ○ small sample size
	  ○ survivorship bias
	  ○ data missing not at random

2.2.4 The impact of bias, incompleteness and lack of representativeness in data on analytical outcomes and interpretation	N/A
2.2.5 Limitations of datasets used in automated and AI-enabled analysis, and potential sources of bias in data collection, preparation, processing and when drawing conclusions	N/A

2.3 Techniques for analysis and insight generation

Teaching content The learner must know and understand	Mandatory additional information
2.3.1 Analytical techniques used to examine prepared datasets	• sorting, filtering and grouping records

DRAFT

Teaching content The learner must know and understand	Mandatory additional information
	• calculating totals, averages, percentages and rates of change, comparing categories and ranking results • identifying trends, patterns and anomalies • selecting techniques in relation to data type and analytical purpose, and interpreting variability and relationships within datasets
2.3.2 The role of automated and AI-enabled analytical systems in supporting pattern identification and insight generation, and the need to interpret outputs critically	N/A
2.3.3 The forms and uses of analytical outputs, and how these inform conclusions and decision-making	• summaries, comparisons, trends and indicators • distributions • forecasts • exception reports • ranked results
2.3.4 The role of interpretation and professional judgement in transforming analytical results into meaningful conclusions	• distinguishing correlation from meaningful relationships • confounding variables • spurious correlation • reverse causation

2.4 Principles of presentation and visual communication

Teaching content The learner must know and understand	Mandatory additional information
2.4.1 How automated visualisation tools may influence interpretation of findings	• the influence of scale, proportion and representation • effects of default or auto-generated chart settings that may not suit the data
2.4.2 The consequences of presenting automated outputs without explaining assumptions, limitations and confidence in the underlying data and analysis	N/A
2.4.3 How workplace setting, audience needs and decision-making purpose influence the selection of presentation formats	N/A
2.4.4 Principles of visual communication that support accurate, transparent, proportionate and non-misleading representation of analysed data findings	N/A

DRAFT

Teaching content The learner must know and understand	Mandatory additional information
2.4.5 The relationship between analytical findings, presentation choices and user interpretation of information	N/A
2.4.6 Inclusive and accessible presentation practices that support understanding by diverse users and audiences	N/A

2.5 Principles of responsible and inclusive data use

Teaching content The learner must know and understand	Mandatory additional information
2.5.1 Policies and procedures relating to data privacy, confidentiality and responsible data use and presentation of insights	• collection, storage and retention of data • access permissions and authorised use of data • anonymisation and protection of personal or sensitive information
2.5.2 Governance and data protection requirements relevant to the use of data in automated and AI-enabled analysis	• lawful and appropriate use of data • protection of personal and sensitive information • transparency and explainability of automated outputs • accountability and human oversight • accuracy, fairness and mitigation of bias in data and analytical processes
2.5.3 The importance of transparency when presenting insights generated and supported by automated and AI-enabled systems	N/A
2.5.4 Principles of inclusive and unbiased data handling that support fair, accurate and responsible interpretation of analytical findings	• recognising potential bias in data collection and representation • considering completeness and representativeness of datasets • avoiding misleading comparisons or visualisations • presenting findings objectively and transparently • considering the needs of diverse users and audiences
2.5.5 Sustainability considerations relating to the preparation, storage and sharing of data outputs	N/A

DRAFT

2.6 Prepare, analyse and present data to support conclusions and decision-making

Teaching content The learner must be able to	Mandatory additional information
2.6.1 Interpret a defined analytical and decision-making purpose	N/A
2.6.2 Examine data from different sources to determine suitability for analysis	N/A
2.6.3 Prepare data for analysis through validation, checking formats and confirming completeness	N/A
2.6.4 Analyse prepared datasets to identify patterns, relationships and trends	N/A
2.6.5 Examine analytical outputs in relation to the defined purpose	N/A
2.6.6 Interpret analytical findings and consider potential sources of bias and limitation in the data	N/A
2.6.7 Draw reasoned conclusions from analysed data	N/A
2.6.8 Select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately	N/A
2.6.9 Ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations	N/A
2.6.10 Communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences	N/A
2.6.11 Document analytical decisions, assumptions and outputs clearly	N/A
2.6.12 Review presented outputs to improve clarity, accessibility and relevance	N/A

Teaching guidance
This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive.
2.1 Characteristics of data structures, sources and quality
2.1.1 The purpose of preparing, analysing, interpreting and presenting data to generate insights that support conclusions and decision-making in workplace contexts could include: • examples of workplace contexts where data-informed decisions matter: ○ reviewing sales performance

DRAFT

Teaching guidance

- monitoring service response times
- evaluating customer satisfaction data.

Worked example of purpose determining what data is needed
A retailer wants to understand how often customers return to the store. Its transaction records contain a customer identifier and the date of each purchase, allowing it to identify how often customers make purchases. However, customers who visit the store without making a purchase do not generate a transaction record. Therefore, the available data can measure repeat purchasing behaviour, but it cannot accurately measure how often customers return to the store.

2.1.2 How data is structured, formatted and defined within datasets from different sources could include:

- examples of granularity mismatch:
  - daily against monthly
  - individual against aggregated
- examples of structural and formatting features that affect how data can be interpreted or compared:
  - field naming and column definitions
  - date formats
  - units of measurement
  - character encoding
- examples of checking a dataset before use:
  - checking fields and columns first
  - confirming the data is complete
  - confirming the data suits the question being asked
- examples of factors that determine whether a dataset is usable:
  - accessibility and availability
  - completeness
  - security and sensitivity of the data.

Worked example of the same information held in different structures
A customer complaint could be recorded as a row in a table containing defined fields such as a product code and refund value. This structured data allows those values to be compared across records. The same complaint could be written as a review in the customer's own words. This unstructured text must be read or processed to identify and analyse key information. Alternatively, a support record could combine labelled fields, such as date and category, with a free-text description, allowing comparison of the defined fields alongside interpretation of the written account.

2.1.3 Data quality issues arising from missing data, duplicate records, inconsistent formats and conflicting values across sources, and their impact on analysis could include:

- examples of the impact of data quality issues on analysis:
  - duplicate records inflating totals and potentially distorting averages
  - missing values left out of a calculation without this being visible
  - inconsistent date formats placing records in the wrong period.

Worked example of data quality issues affecting a finding
Sales data from two branches are combined. The dataset contains duplicate orders, missing refund values and inconsistent date formats. Until these issues are identified and resolved, the analysis may be misleading. Duplicate orders may make revenue appear too high, while inconsistent date formats

DRAFT

Teaching guidance
may place sales in the wrong month. Using this information to plan stock could result in the business ordering more stock than needed or ordering it at the wrong time.

2.1.4 Methods used to validate and prepare data prior to analysis through checking formats and data types, confirming completeness, verifying value ranges and resolving inconsistencies could include:
 	
• examples of common data types:
  ○ text (string)
  ○ whole numbers (integer)
  ○ numbers with fractional parts (float or decimal)
  ○ dates and times
  ○ true or false values (Boolean)
  ○ categories, such as product type or customer group (categorical)
• examples of validation methods:
  ○ checking that a numeric field holds numbers rather than text
  ○ checking for blank values in fields that must be completed
  ○ identifying values outside a plausible range, such as a negative age
  ○ agreeing a single format for dates or names before sources are combined.

2.1.5 The role of metadata, field definitions and documentation in supporting analysis, transparency, accountability and correct interpretation of analysed outputs could include:
 	
• examples of metadata:
  ○ when a dataset was created and last updated
  ○ who produced it and for what purpose
  ○ the source of the data and how it was collected
• examples of field definitions:
  ○ what a field contains, its data type and the format in which values are recorded
  ○ what a value means where it is coded or abbreviated
• examples of documentation:
  ○ a record of how data was prepared, including what was cleaned, removed or transformed
  ○ assumptions made and known limitations of the dataset
• examples of reasons for recording this information:
  ○ allowing someone else to verify how a conclusion was reached
  ○ showing what the data does and does not support.
 	
Worked example of metadata, field definitions and documentation used together
A report states that the average customer age is 45. To interpret it correctly a learner needs to know where the customer data came from (metadata), whether age means current age or age at registration (field definitions), and how the average was calculated (documentation).

2.2 Methods of preparing and combining datasets

2.2.1 How combining datasets from different sources can reveal relationships and insights not visible when sources are analysed separately could include:
 	
• examples of granularity mismatch:
  ○ daily transactions against monthly totals
  ○ individual customer records against store or regional summaries
• examples of duplicate entities across sources:
  ○ differences in how customer details are entered, such as ‘John Smith’ in one system and ‘J. Smith’ in another, making it difficult to determine whether the records refer to the same person

DRAFT

Teaching guidance
○ one record entered manually and another imported automatically ○ the same product under different codes • examples of column and field mismatch: ○ a column named ‘outcome’ against one named ‘complaint outcome’ ○ differences in capitalisation or trailing spaces • examples of differing data entry rules between sources: ○ a closed complaint carrying no closure date, where one source enforces the rule and another does not • examples of the effects of unresolved combination risks: ○ duplicate records skewing averages and totals ○ conflicting values producing unreliable conclusions ○ results that do not capture what was intended. **Worked example of combining datasets to answer a workplace question** A retailer stores sales records and returns records separately. By matching the two datasets using a shared transaction identifier, the retailer can calculate the return rate for each product, which neither dataset shows on its own. However, if a transaction identifier is missing or does not match, the return cannot be linked to the original sale. If unmatched returns are excluded from the calculation, the calculated return rate may be lower than the actual rate.
2.2.2 The relationship between data preparation, analytical methods and the reliability of conclusions could include: • examples of preparation choices that can change the conclusions drawn from the same dataset: ○ rounding ○ aggregation methods • examples of stages in preparing data for analysis: ○ cleaning ○ transforming ○ combining.
2.2.3 The relationship between data quality, analytical approach, data limitations, uncertainty and confidence in conclusions No additional teaching guidance is provided for this teaching content.
2.2.4 The impact of bias, incompleteness and lack of representativeness in data on analytical outcomes and interpretation could include: • examples of impact on outcomes and interpretation: ○ a finding that is true for one group being applied to every group ○ a trend appearing or disappearing depending on which records are included ○ confidence in a conclusion being higher than the data supports. **Worked example of unrepresentative data affecting a conclusion** A business surveys customers online and finds most prefer to be contacted by email. Customers who do not use the internet were never asked, so the finding reflects online customers rather than all customers. Moving all contact to email on that basis would leave part of the customer base unreached.
2.2.5 Limitations of datasets used in automated and AI-enabled analysis, and potential sources of bias in data collection, preparation, processing and when drawing conclusions could include:

DRAFT

Teaching guidance

- examples of where bias can enter automated analysis:
  - data collection, where the data collected does not represent the population or events being studied
  - data preparation, where records with missing or incomplete values are removed and the missing data is not distributed randomly across the population
  - data processing, where an automated system is trained on historical data that reflects previous bias
  - drawing conclusions, where results are accepted without checking whether the data and results are representative of the relevant groups.

Worked example of bias carrying into an automated output
The online survey data from 2.2.4 is used to train an automated tool to predict each customer's preferred contact method. Because the survey is completed only by customers who engage online, customers who prefer or rely on other contact methods are under-represented. As a result, the tool may learn to favour email and recommend it for customers who have never used email to communicate with the retailer.

2.3 Techniques for analysis and insight generation

2.3.1 Analytical techniques used to examine prepared datasets could include:

- examples of foundational statistical techniques appropriate at this level:
  - measures of central tendency and spread
  - identifying trends over time, for example, using moving averages
  - recognising patterns and anomalies against expected ranges.

Worked example of choosing a technique to suit the data
A teacher wants to examine whether hours spent studying are associated with exam scores. A scatter graph can help show whether the relationship appears broadly linear and whether there are unusual values. Where appropriate, Pearson correlation can then summarise the strength and direction of the linear relationship. This shows an association; it does not establish that studying for longer caused higher scores.

2.3.2 The role of automated and AI-enabled analytical systems in supporting pattern identification and insight generation, and the need to interpret outputs critically could include:

- examples of automated and AI-enabled analytical tools:
  - automated dashboards
  - anomaly detection tools
  - predictive models
- examples of why outputs need critical interpretation:
  - a pattern that reflects how the data was collected rather than what it describes
  - a prediction based on training data that no longer reflects current conditions.

Worked example of an automated system identifying a pattern
An anomaly detection tool flags an unusual rise in returns for one product. The tool identifies the increase but does not establish its cause. Possible explanations include a faulty batch, a misleading product description or a change in returns policy. In this example, determining the cause requires further investigation using information that is not available to the tool.

DRAFT

Teaching guidance
2.3.3 The forms and uses of analytical outputs, and how these inform conclusions and decision-making No additional teaching guidance is provided for this teaching content.
2.3.4 The role of interpretation and professional judgement in transforming analytical results into meaningful conclusions No additional teaching guidance is provided for this teaching content.
2.4 Principles of presentation and visual communication

2.4.1 How automated visualisation tools may influence interpretation of findings could include:
 	
• examples of default or auto-generated settings that may not suit the data:
  ○ truncated axes
  ○ automatic chart type selection
  ○ automatic number formatting, such as a value displaying as a percentage or currency
  ○ default colour schemes that may not meet accessibility needs
  ○ automatically selected date ranges.

2.4.2 The consequences of presenting automated outputs without explaining assumptions, limitations and confidence in the underlying data and analysis could include:
 	
• examples of what is often left unexplained:
  ○ assumptions, such as assuming that future demand will follow patterns seen in historical data
  ○ limitations, such as the data covering only some customers, products or time periods
  ○ confidence, such as showing a prediction without explaining how likely it is to be correct.
 	
Worked example of an automated output presented without its assumptions
An automated forecast predicts next month's sales as a single figure. It assumes demand will continue to follow previous monthly patterns, but this assumption is not explained when the forecast is shared. A seasonal drop in demand is expected but has not been accounted for. If a manager treats the forecast as certain, they may order more stock than can be sold.

2.4.3 How workplace setting, audience needs and decision-making purpose influence the selection of presentation formats could include:
 	
• examples of presentation formats matched to audience:
  ○ dashboards
  ○ written reports
  ○ slide summaries
  ○ infographics.

2.4.4 Principles of visual communication that support accurate, transparent, proportionate and non-misleading representation of analysed data findings could include:
 	
• examples of these principles in practice:
  ○ accurate, where values and labels match the underlying data
  ○ transparent, where the source and time period are stated
  ○ proportionate, where the visual scale reflects the actual size of differences in the data
  ○ non-misleading, where comparisons use the same measures and scales so they can be compared fairly.

DRAFT

Teaching guidance
Worked example of an accurate chart that is not proportionate Two bar charts show the same monthly sales of 480 and 500 units. In one chart, the vertical axis starts at 470, making the difference appear much larger than it is. In the other, the axis starts at zero, so the bars appear much closer in height. Both charts use accurate data, but the second gives a more proportionate visual representation of the increase of approximately 4.2%.

2.4.5 The relationship between analytical findings, presentation choices and user interpretation of information could include:
 	
• examples of presentation choices that affect how findings are read:
  ○ ordering of categories influencing perceived importance
  ○ level of summarisation affecting the perceived certainty of a finding.

2.4.6 Inclusive and accessible presentation practices that support understanding by diverse users and audiences. No additional teaching guidance is provided for this teaching content.
2.5 Principles of responsible and inclusive data use

2.5.1 Policies and procedures relating to data privacy, confidentiality and responsible data use and presentation of insights could include:
 	
• examples of access and retention controls:
  ○ defined retention schedules
  ○ read-only permissions
• examples of storing data securely:
  ○ using an approved document management system with access permissions set to match the sensitivity of the data
  ○ matching the storage to the sensitivity of the data, with more sensitive data held in a controlled repository
• examples of collection and retention practices:
  ○ how data is collected, such as forms, sensors or system logs
  ○ how long data is kept, and the risks of retaining it longer than needed.

2.5.2 Governance and data protection requirements relevant to the use of data in automated and AI-enabled analysis. No additional teaching guidance is provided for this teaching content.

2.5.3 The importance of transparency when presenting insights generated and supported by automated and AI-enabled systems could include:
 	
• examples of what transparency about the process covers:
  ○ which system was used and for which part of the analysis
  ○ what a person checked before the findings were shared
  ○ which parts of a finding came from the system and which from a person.
 	
Worked example of presenting an AI-assisted analysis
Two reports state that complaints about delivery increased in the last quarter. One explains that an AI tool grouped complaints by theme and that a person checked a sample of those groupings. The other

DRAFT

Teaching guidance
provides no information about how the finding was produced or checked. The first report gives readers context to understand how the finding was reached and question the process used.
2.5.4 Principles of inclusive and unbiased data handling that support fair, accurate and responsible interpretation of analytical findings **Worked example of recognising under-representation when interpreting findings** A customer survey indicates that most respondents are satisfied. However, further analysis identifies that very few responses came from female customers. The company explains this under-representation when presenting the findings and avoids claiming that the results represent all customers.
2.5.5 Sustainability considerations relating to the preparation, storage and sharing of data outputs No additional teaching guidance is provided for this teaching content.
2.6 Prepare, analyse and present data to support conclusions and decision-making
2.6.1 Interpret a defined analytical and decision-making purpose No additional teaching guidance is provided for this teaching content.
2.6.2 Examine data from different sources to determine suitability for analysis No additional teaching guidance is provided for this teaching content.
2.6.3 Prepare data for analysis through validation, checking formats and confirming completeness No additional teaching guidance is provided for this teaching content.
2.6.4 Analyse prepared datasets to identify patterns, relationships and trends No additional teaching guidance is provided for this teaching content.
2.6.5 Examine analytical outputs in relation to the defined purpose No additional teaching guidance is provided for this teaching content.
2.6.6 Interpret analytical findings and consider potential sources of bias and limitation in the data No additional teaching guidance is provided for this teaching content.
2.6.7 Draw reasoned conclusions from analysed data No additional teaching guidance is provided for this teaching content.
2.6.8 Select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately No additional teaching guidance is provided for this teaching content.
2.6.9 Ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations No additional teaching guidance is provided for this teaching content.

DRAFT

Teaching guidance
2.6.10 Communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences No additional teaching guidance is provided for this teaching content.

2.6.11 Document analytical decisions, assumptions and outputs clearly could include:
 	
• examples of documentation conventions for an analytical record:
  ○ the choices made, such as which technique was used and why
  ○ the assumptions relied on
  ○ the outputs produced and where they are held.
 	
Worked example of an analytical record in use
An analyst documents how an average was calculated, the assumptions used and where the output is stored. The record explains that incomplete records were removed before calculation and that the analysis assumes all branches reported data for the same period. Another analyst reviewing the work later can see how the figures were produced and why the average may differ from an earlier report without needing to repeat the analysis.

2.6.12 Review presented outputs to improve clarity, accessibility and relevance No additional teaching guidance is provided for this teaching content.

Transferable skills
The following transferable skills have been integrated into the content for work-related purposes: • **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.

Workplace behaviours
No workplace behaviours have been identified within this theme.

DRAFT

Theme 3 Principles of communication, problem solving and ethical practice

Theme summary
The aim of this theme is to provide the conceptual foundation for how digital work is carried out with others and what responsible practice involves. It covers communication and collaboration in technical contexts, the principles underpinning problem solving and solution design, and the implications of using automated and AI-enabled systems alongside the legal, ethical and sustainability considerations relevant to digital practice.

Assessment			
Assessment by examination (AbE) and non-exam assessment (NEA)			
Mandatory The teaching content and mandatory additional information must be covered by the tutor during the delivery of this qualification.	**Assessment reference** Refer to the scheme of assessment in Section 1.	**Level 3**	**60 GLH** Refer to the scheme of assessment in Section 1 for AbE and NEA assessment durations.

3.1 Principles of communication and collaboration in technical contexts

Teaching content The learner must know and understand	**Mandatory additional information**
3.1.1 The role of communication in technical support	• how information is gathered, interpreted and conveyed to support accurate identification and resolution of issues and effective service delivery
3.1.2 How communication approaches influence clarity, efficiency and user experience	• the need to adapt communication to meet diverse user needs • to distinguish between communication-based support and technical troubleshooting activities
3.1.3 Principles of professional, ethical, clear and responsible communication when handling technical information	• accuracy and consistency of information • use of appropriate technical and non-technical language • maintaining confidentiality and respecting privacy • adapting communication to audience needs • responding appropriately to user queries and expectations
3.1.4 The role of collaboration in developing digital solutions	• how different roles, perspectives and forms of expertise contribute to decision-making and the quality of proposed solutions

DRAFT

Teaching content The learner must know and understand	Mandatory additional information
	• how structured approaches to collaborative working support effective and consistent outcomes

3.1.5 How user needs are identified, interpreted and translated into digital solution designs	• the role of feedback, iteration and shared understanding in refining solutions
	• methods of gathering and acting on feedback:
	  ○ user testing
	  ○ prototyping and review cycles
	  ○ requirement traceability

3.2 Considerations in problem solving, automation and ethical practice

Teaching content The learner must know and understand	Mandatory additional information
3.2.1 The implications of using automated and AI-enabled systems in decision-making	• limitations • bias • the need for human oversight • limitations and accuracy of automated outputs • bias and fairness in automated decision-making • human oversight and validation of automated outputs
3.2.2 Principles of problem solving, programming logic and digital solution design, and structured approaches used to develop, test and refine digital solutions	• abstraction • decomposition • sequencing • selection • iteration
3.2.3 The role of prompts and structured inputs in generating outputs from automated and AI-enabled systems	• how prompt design influences the relevance, accuracy and limitations of generated outputs • the broader social and ethical implications of automated and AI-enabled systems and their outputs • principles of prompt engineering • methods of verifying generated outputs • attribution of AI-assisted work • workforce impact of automated and AI-enabled systems
3.2.4 Ethical, legal and sustainability considerations relevant to digital practice	• intellectual property rights, ownership, attribution • the responsible use of automated and AI-enabled systems and their outputs

DRAFT

Teaching content The learner must know and understand	Mandatory additional information

	• legal requirements relevant to digital practice:
	  ○ UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
	  ○ Computer Misuse Act 1990
	  ○ Copyright, Designs and Patents Act 1988
	  ○ Equality Act 2010
	• relevant workplace codes of conduct and information security policies

3.2.5 The influence of constraints on collaborative decision-making and digital solution design, and the importance of inclusive and responsible collaboration in achieving effective outcomes	• technical, organisational and resource factors

Teaching guidance

This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive.

Some concepts in this theme also appear in the themes that include skills. This theme provides the understanding; those themes are where learners apply it.

3.1 Principles of communication and collaboration in technical contexts

3.1.1 The role of communication in technical support could include:

- examples of gathering and conveying information in technical support:
  - questioning techniques
  - active listening
  - structured handover formats
- examples of what a communication log or record is used for:
  - capturing what was discussed, what changed and what actions followed
  - allowing recurring questions to be answered by reference to earlier exchanges.

3.1.2 How communication approaches influence clarity, efficiency and user experience could include:

- examples of adapting tone and language for different audiences:
  - using non-technical language where appropriate
  - explaining the same fix to a technical colleague and to a non-technical customer
  - writing a handover note and speaking to a distressed user.

3.1.3 Principles of professional, ethical, clear and responsible communication when handling technical information

No additional teaching guidance is provided for this teaching content.

DRAFT

Teaching guidance

3.1.4 The role of collaboration in developing digital solutions could include:
 	
• examples of collaborative approaches:
  ○ pair programming
  ○ structured design reviews
  ○ daily stand-ups
  ○ RACI matrix role clarification
  ○ prototyping and reviewing.
 	
Worked example of RACI role clarification
In a team building a new website feature, the developers are responsible for building it, the team lead is accountable for sign-off, the customer support manager who requested it is consulted, and the wider support team is informed once it goes live.

3.1.5 How user needs are identified, interpreted and translated into digital solution designs No additional teaching guidance is provided for this teaching content.
3.2 Considerations in problem solving, automation and ethical practice

3.2.1 The implications of using automated and AI-enabled systems in decision-making could include:
 	
• examples of limitations in practice:
  ○ recognising when a decision is being automated at all
• examples of bias in practice:
  ○ questioning whether training data represents the whole population or the sample it is applied to
• examples of proportionate human oversight:
  ○ matching the level of checking to the stakes of the decision.

3.2.2 Principles of problem solving, programming logic and digital solution design, and structured approaches used to develop, test and refine digital solutions No additional teaching guidance is provided for this teaching content.

3.2.3 The role of prompts and structured inputs in generating outputs from automated and AI-enabled systems could include:
 	
• examples of social and ethical implications:
  ○ bias and discrimination, where systems use training data that reflects existing social inequalities
  ○ privacy, including what personal data is collected, how it is used and how long it is kept
  ○ surveillance, such as using facial recognition to monitor people
  ○ accountability and responsibility, including who should explain and address incorrect outputs or decisions
  ○ misinformation, such as fabricated news or deepfakes
  ○ transparency, such as explaining why an automated system rejected a loan application
  ○ environmental impact, such as the energy used to train and operate AI systems
• examples of workforce impact:
  ○ tasks previously done by people becoming automated
  ○ new roles in checking, maintaining and supervising automated systems
  ○ different skills needed to work alongside automated systems.

DRAFT

Teaching guidance
3.2.4 Ethical, legal and sustainability considerations relevant to digital practice could include: • examples of organisational codes of conduct, such as equality and inclusion or confidentiality, and how these help an organisation operate legally and ethically, which may vary between sectors • examples of professional body codes of conduct, such as those of BCS, The Chartered Institute for IT.

3.2.5 The influence of constraints on collaborative decision-making and digital solution design, and the importance of inclusive and responsible collaboration in achieving effective outcomes could include:
 	
• examples of technical constraints:
  ○ legacy systems unable to support a required capability, for example real-time data
  ○ compatibility with systems already in use
• examples of organisational constraints:
  ○ regulatory and compliance requirements, particularly in sectors such as financial services or healthcare
  ○ lengthy approval processes
• examples of resource constraints:
  ○ skills and capability available within the team
  ○ budget, people, equipment and infrastructure
  ○ fixed deadlines set by external stakeholders.
• examples of inclusive and responsible collaboration:
  ○ involving all affected stakeholders in decisions, including non-technical colleagues and end users, rather than only the technical team
  ○ making sure constraints known to one part of the team are shared with the whole team before decisions are made
  ○ recognising the impact of a decision on people who are not in the room, including users with accessibility needs
  ○ being transparent about the reasons behind a decision so it can be understood and challenged by others
  ○ respecting different perspectives and using accessible communication.

Transferable skills
No transferable skills have been identified within this theme.

Workplace behaviours
No workplace behaviours have been identified within this theme.

DRAFT

Theme 4 Cyber security operations and response

Theme summary			
The aim of this theme is to develop the knowledge, understanding and skills needed to apply security protocols, interpret security-related system information, and detect and escalate cyber security concerns in line with defined procedures.			
Assessment			
Assessment by examination (AbE) and non-exam assessment (NEA)			
Mandatory The teaching content and mandatory additional information must be covered by the tutor during the delivery of this qualification.	**Assessment reference** Refer to the scheme of assessment in Section 1.	**Level 3**	**80 GLH** Refer to the scheme of assessment in Section 1 for AbE and NEA assessment durations.

4.1 Purpose of security principles, controls and policies

Teaching content The learner must know and understand	**Mandatory additional information**

4.1.1 Authentication requirements, access controls, update procedures and data protection measures used to protect digital systems and services	• the relationship between authentication strength, usability and security risk
	• principles of least privilege
	• principles of secure system design:
	  ○ defence in depth
	  ○ separation of duties
	  ○ fail secure
	  ○ secure by design

4.1.2 Policies relating to acceptable use, access control, data handling and incident reporting, and their role in guiding secure practice	• acceptable use of systems, devices and services • user authentication and access permissions • secure storage, sharing and disposal of data • reporting and escalation of suspected security incidents
4.1.3 The relationship between security controls, user behaviour and system vulnerabilities	N/A
4.1.4 Policies and procedures relating to privacy, confidentiality and responsible handling of security-related information	• storing information securely • restricting access to authorised users • transmitting information appropriately • reporting concerns through defined procedures

DRAFT

4.2 Characteristics of threats and risk identification

Teaching content The learner must know and understand	Mandatory additional information
4.2.1 Common cyber security threats	• phishing • social engineering • malware • ransomware • unauthorised access attempts • suspicious network behaviour • data loss incidents
4.2.2 The relationship between system activity, security-related information and potential cyber security concerns	• uncertainty in interpretation and the need for professional judgement
4.2.3 The role of baseline system behaviour in identifying deviations and potential threats	N/A
4.2.4 The implications of different types of cyber threats and the impact of delayed identification and escalation	N/A

4.3 Interpreting security-related system information

Teaching content The learner must know and understand	Mandatory additional information
4.3.1 The use of system logs, alert notifications and account activity records to identify indicators of potential cyber security concerns	• correlation of multiple indicators • distinguishing normal system variation from anomalous behaviour • methods of establishing expected system behaviour: ○ time-of-day and seasonal baselining

4.4 Role of automated and AI-enabled detection

Teaching content The learner must know and understand	Mandatory additional information
4.4.1 The importance of accurate interpretation of system information, awareness of false positives and misinterpretation of automated alerts, and the limitations of automated and AI-enabled detection systems	N/A
4.4.2 The role of automated and AI-enabled detection systems in identifying potential cyber security concerns, and the need to interpret, validate and act on outputs appropriately	N/A

DRAFT

4.5 Principles of responsible and sustainable practice

Teaching content The learner must know and understand	Mandatory additional information
4.5.1 Energy efficiency, data retention management and secure device lifecycle practices relevant to cyber security	N/A

4.6 Apply security procedures and interpret system information to identify and escalate concerns

Teaching content The learner must be able to	Mandatory additional information
4.6.1 Apply authentication requirements, access controls, update procedures and data protection measures to digital systems	N/A
4.6.2 Apply configuration actions relating to user accounts, permissions and security settings in line with defined security procedures	N/A
4.6.3 Apply procedures for secure access, authentication and system use	N/A
4.6.4 Review security-related information to identify slow response times, repeated errors, failed updates and connectivity interruptions, and what these indicate about system quality	N/A
4.6.5 Recognise signs of unexpected and anomalous system activity	N/A
4.6.6 Use log files, monitoring dashboards and system alerts to view and interpret security-related information	N/A
4.6.7 Record observations clearly and accurately	N/A
4.6.8 Escalate potential cyber security concerns in line with security procedures	N/A
4.6.9 Select and apply protective actions to systems in response to identified risks and system information	N/A
4.6.10 Communicate potential security concerns clearly to others	N/A
4.6.11 Handle security-related information in line with policies and procedures for privacy and confidentiality	N/A

DRAFT

Teaching guidance
This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive.
4.1 Purpose of security principles, controls and policies

4.1.1 Authentication requirements, access controls, update procedures and data protection measures used to protect digital systems and services could include:
 	
• examples of physical access controls:
  ○ locks
  ○ access cards
  ○ biometric systems
• examples of access control methods:
  ○ RBAC
  ○ MAC
• examples of authentication requirements:
  ○ password and PIN requirements (for example, complexity)
  ○ MFA
• examples of technical controls covered by NCSC Cyber Essentials:
  ○ firewalls, controlling network traffic to help prevent unauthorised access
  ○ secure configuration, applying secure settings to devices, software and applications
  ○ user access control, ensuring users have only the access they need
  ○ malware protection, protecting devices and systems against malicious software
  ○ security update management, keeping software and devices updated to address security vulnerabilities
• examples of how security controls support the CIA triad:
  ○ confidentiality, restricting access to information to authorised users
  ○ integrity, protecting information against unauthorised changes
  ○ availability, supporting access to information and systems when authorised users need them.
 	
Worked example of authentication and access control as separate steps
A member of staff signs in successfully with a password and a code sent to their phone, but cannot open a folder of payroll records. Signing in confirmed who they are; their permissions determine what they can access, and payroll is restricted to the finance team.

4.1.2 Policies relating to acceptable use, access control, data handling and incident reporting, and their role in guiding secure practice No additional teaching guidance is provided for this teaching content.

4.1.3 The relationship between security controls, user behaviour and system vulnerabilities could include:
 	
• examples of security controls:
  ○ firewalls
  ○ antivirus
  ○ encryption
  ○ intrusion detection and prevention
  ○ monitoring
  ○ user access policies and procedures
• examples of user behaviour that affects security:
  ○ password practices

DRAFT

Teaching guidance

- responding to phishing attempts
- following or bypassing policies and controls
- reporting incidents

- examples of system vulnerabilities:
  - unpatched software
  - misconfigured systems
  - insecure or legacy applications
  - weak authentication
- examples of reducing the attack surface:
  - closing unnecessary network ports
  - disabling unused services
  - removing unused accounts
  - removing access permissions no longer needed.

Worked example of user behaviour affecting a security control
An employee enters a secure office using their access card. An unauthorised person follows closely behind, and the employee holds the door open for them. The person enters without using an access card. By allowing someone to enter without checking their authorisation, the employee undermines the protection provided by the access control.

4.1.4 Policies and procedures relating to privacy, confidentiality and responsible handling of security-related information

No additional teaching guidance is provided for this teaching content.

4.2 Characteristics of threats and risk identification

4.2.1 Common cyber security threats

Worked example of the listed threats occurring within one incident
A member of staff receives an email appearing to come from their IT department, asking them to confirm their password through a link. The email is a phishing attempt, and the employee enters their password on the linked page. The stolen password is then used to gain unauthorised access to the account. Monitoring identifies logins at unusual times and suspicious network behaviour involving large file transfers. Customer records are copied out of the organisation, resulting in a data loss incident.

4.2.2 The relationship between system activity, security-related information and potential cyber security concerns could include:

- examples of interpretation proving wrong on first reading:
  - unusual system processes assumed to indicate an intrusion, later found to be an outdated component requiring a patch
  - a legitimate internal email reported as phishing during a security awareness campaign, where prior warning led to over-cautious interpretation
- examples of deciding when to escalate under uncertainty in line with defined procedures:
  - when the potential impact is high, such as an unusual login involving an account with access to sensitive customer data
  - when a concern is beyond a member of staff's knowledge or authority to investigate, such as a suspicious email they refer to IT
  - when several warning signs occur together, such as repeated failed login attempts followed by an unexpected large data transfer.

Teaching guidance
4.2.3 The role of baseline system behaviour in identifying deviations and potential threats No additional teaching guidance is provided for this teaching content.
4.2.4 The implications of different types of cyber threats and the impact of delayed identification and escalation No additional teaching guidance is provided for this teaching content.
4.3 Interpreting security-related system information

4.3.1 The use of system logs, alert notifications and account activity records to identify indicators of potential cyber security concerns could include:
 	
• examples of the effects of alert fatigue on accurate interpretation:
  ○ desensitisation to false positives
  ○ genuine concerns being missed or dismissed.

4.4 Role of automated and AI-enabled detection

4.4.1 The importance of accurate interpretation of system information, awareness of false positives and misinterpretation of automated alerts, and the limitations of automated and AI-enabled detection systems could include:
 	
• examples of errors in automated detection:
  ○ false positives, where normal activity triggers an alert
  ○ false negatives, where genuine malicious activity triggers no alert
• examples of limitations of automated and AI-enabled detection:
  ○ activity that falls outside the patterns the system was set up to recognise
  ○ normal changes in behaviour, such as a new device or a busier period, being treated as suspicious.
 	
Worked example of a false positive
A monitoring system raises an automated alert warning that an account may be compromised, based on unusual login activity. A technician investigates and confirms that the activity was the genuine user signing in from a new device. Blocking access solely on the basis of the alert would have prevented legitimate use.

4.4.2 The role of automated and AI-enabled detection systems in identifying potential cyber security concerns, and the need to interpret, validate and act on outputs appropriately No additional teaching guidance is provided for this teaching content.
4.5 Principles of responsible and sustainable practice
4.5.1 Energy efficiency, data retention management and secure device lifecycle practices relevant to cyber security No additional teaching guidance is provided for this teaching content.
4.6 Apply security procedures and interpret system information to identify and escalate concerns

DRAFT

Teaching guidance
4.6.1 Apply authentication requirements, access controls, update procedures and data protection measures to digital systems No additional teaching guidance is provided for this teaching content.
4.6.2 Apply configuration actions relating to user accounts, permissions and security settings in line with defined security procedures No additional teaching guidance is provided for this teaching content.
4.6.3 Apply procedures for secure access, authentication and system use No additional teaching guidance is provided for this teaching content.
4.6.4 Review security-related information to identify slow response times, repeated errors, failed updates and connectivity interruptions, and what these indicate about system quality No additional teaching guidance is provided for this teaching content.
4.6.5 Recognise signs of unexpected and anomalous system activity No additional teaching guidance is provided for this teaching content.
4.6.6 Use log files, monitoring dashboards and system alerts to view and interpret security-related information No additional teaching guidance is provided for this teaching content.
4.6.7 Record observations clearly and accurately No additional teaching guidance is provided for this teaching content.
4.6.8 Escalate potential cyber security concerns in line with security procedures No additional teaching guidance is provided for this teaching content.
4.6.9 Select and apply protective actions to systems in response to identified risks and system information No additional teaching guidance is provided for this teaching content.
4.6.10 Communicate potential security concerns clearly to others No additional teaching guidance is provided for this teaching content.
4.6.11 Handle security-related information in line with policies and procedures for privacy and confidentiality No additional teaching guidance is provided for this teaching content.

Transferable skills
The following transferable skills have been integrated into the content for work-related purposes:

DRAFT

Transferable 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.

Workplace behaviours
No workplace behaviours have been identified within this theme.

DRAFT

Theme 5 Digital systems configuration and assurance

Theme summary
The aim of this theme is to develop the knowledge, understanding and skills needed to prepare and configure digital systems in response to defined user requirements, and to confirm that systems meet defined functionality, usability, security and performance requirements. Activities may be undertaken in realistic, controlled, non-live or simulated digital environments where appropriate.

Assessment			
Non-exam assessment (NEA)			
Optional Where this optional theme is selected, the teaching content and mandatory additional information must be covered by the tutor during the delivery of this qualification.	**Assessment reference** Refer to the scheme of assessment in Section 1.	**Level 3**	**80 GLH** Refer to the scheme of assessment in Section 1 for NEA assessment durations.

5.1 System configuration principles

Teaching content The learner must know and understand	**Mandatory additional information**
5.1.1 The role of system dependencies and component compatibility in ensuring reliable system operation	N/A
5.1.2 The impact of system configuration on performance efficiency and resource utilisation	N/A
5.1.3 The role of controlled, non-live, simulated and training environments in supporting safe and effective configuration practice	N/A
5.1.4 The role of digital tools in supporting system preparation, configuration and checking activities	N/A
5.1.5 The role of clear documentation and communication in supporting accurate, consistent and effective system preparation	N/A
5.1.6 The impact of responsible, inclusive and secure configuration practices, and how accessible configuration supports diverse users and reduces barriers to digital participation	N/A

DRAFT

5.1.7 The importance of maintaining system integrity through responsible updates, permissions and security settings	N/A

5.2 Purpose and methods of testing and quality assurance

Teaching content The learner must know and understand	**Mandatory additional information**
5.2.1 The purpose of testing digital systems and the role of quality assurance in maintaining system performance, security and service reliability	N/A
5.2.2 Categories of testing used in workplace contexts that address system functionality, performance, usability, accessibility and security-related behaviours	N/A
5.2.3 Methods used to assess system behaviour through comparison of observed outputs with expected outcomes, interpretation of system logs, alerts and performance indicators, and identification of patterns and recurring issues	N/A
5.2.4 The role of workplace policies, standards and compliance requirements in defining testing scope and quality assurance expectations	N/A
5.2.5 The role of recording and documenting test findings accurately and consistently to support review, accountability and improvement decisions	N/A

5.3 Impact of usability, accessibility and reliability

Teaching content The learner must know and understand	**Mandatory additional information**
5.3.1 The impact of system performance, reliability and security issues on user experience, productivity and service continuity	N/A
5.3.2 Principles of usability and accessibility and their relevance to system performance, reliability and security for diverse users	• the relationship between interface design, interaction patterns and user effectiveness
5.3.3 The contribution of inclusive and accessible testing practices to reliable digital systems for diverse users	N/A

DRAFT

5.3.4 Environmental and sustainability considerations associated with system performance and efficient use of digital resources	N/A

5.4 Role of digital tools and AI-enabled testing

Teaching content The learner must know and understand	**Mandatory additional information**
5.4.1 The role of contemporary digital tools in supporting test planning, identification of patterns in system behaviour and summarisation of findings	N/A
5.4.2 The role of digital tools and automated and AI-enabled systems in supporting system configuration, testing and identification of patterns in system behaviour, and the need to review outputs to ensure accuracy and suitability	N/A

5.5 Principles of secure and responsible operation

Teaching content The learner must know and understand	**Mandatory additional information**
5.5.1 Policies relating to data protection, privacy and acceptable system use, and their role in guiding configuration practice	• access permissions and user account management • secure configuration and update practices • protection of personal and sensitive information • acceptable use of systems, devices and services

5.6 Configure and test digital systems to confirm readiness for use

Teaching content The learner must be able to	**Mandatory additional information**
5.6.1 Interpret user and system requirements to determine configuration needs and the scope and focus of testing	N/A
5.6.2 Prepare and configure digital systems to meet defined needs	N/A
5.6.3 Adjust configuration settings relating to user access, connectivity, storage and security to support system functionality and accessibility	N/A

DRAFT

Teaching content The learner must be able to	**Mandatory additional information**
5.6.4 Carry out structured tests to confirm system functionality, performance, stability and security-related behaviours	N/A
5.6.5 Assess system usability and accessibility against stated user needs	N/A
5.6.6 Review system behaviour and outputs to identify deviations from expected outcomes and apply structured fault-finding approaches where required	N/A
5.6.7 Record and compare test outcomes against requirements using accurate terminology and structured formats	N/A
5.6.8 Evaluate test outcomes in relation to defined requirements to determine whether systems are ready for use or require further adjustment	N/A
5.6.9 Identify and correct configuration settings related to user access, connectivity, storage and security that do not meet defined user requirements	N/A
5.6.10 Apply routine checks to confirm systems are ready for use	• user access and authentication • connectivity and network access • storage availability • software updates and security settings • expected system functionality and performance
5.6.11 Apply policies relating to configuration and data protection requirements	• secure configuration • access permissions • protection of personal information • software updates
5.6.12 Document configuration decisions clearly	N/A
5.6.13 Communicate configuration outcomes clearly and respond to queries in line with workplace procedures	N/A
5.6.14 Maintain system integrity through responsible configuration practices, updates, permissions and security settings	N/A

Teaching guidance
This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive.

DRAFT

Teaching guidance
5.1 System configuration principles
5.1.1 The role of system dependencies and component compatibility in ensuring reliable system operation No additional teaching guidance is provided for this teaching content.
5.1.2 The impact of system configuration on performance efficiency and resource utilisation No additional teaching guidance is provided for this teaching content.
5.1.3 The role of controlled, non-live, simulated and training environments in supporting safe and effective configuration practice No additional teaching guidance is provided for this teaching content.

5.1.4 The role of digital tools in supporting system preparation, configuration and checking activities could include:
 	
• examples of digital tools used to support configuration and checking:
  ○ configuration management tools
  ○ system monitoring and reporting tools
  ○ automated checking or scripting tools.

5.1.5 The role of clear documentation and communication in supporting accurate, consistent and effective system preparation No additional teaching guidance is provided for this teaching content.
5.1.6 The impact of responsible, inclusive and secure configuration practices, and how accessible configuration supports diverse users and reduces barriers to digital participation No additional teaching guidance is provided for this teaching content.

5.1.7 The importance of maintaining system integrity through responsible updates, permissions and security settings could include:
 	
• examples of what each configuration area covers when preparing a system for use:
  ○ user access, including accounts, permissions and authentication settings
  ○ connectivity, including network access and service availability
  ○ storage, including capacity, location and backup settings
  ○ security settings, including update status and protection measures.

5.2 Purpose and methods of testing and quality assurance
5.2.1 The purpose of testing digital systems and the role of quality assurance in maintaining system performance, security and service reliability No additional teaching guidance is provided for this teaching content.
5.2.2 Categories of testing used in workplace contexts that address system functionality, performance, usability, accessibility and security-related behaviours No additional teaching guidance is provided for this teaching content.

DRAFT

Teaching guidance
5.2.3 Methods used to assess system behaviour through comparison of observed outputs with expected outcomes, interpretation of system logs, alerts and performance indicators, and identification of patterns and recurring issues No additional teaching guidance is provided for this teaching content.
5.2.4 The role of workplace policies, standards and compliance requirements in defining testing scope and quality assurance expectations No additional teaching guidance is provided for this teaching content.
5.2.5 The role of recording and documenting test findings accurately and consistently to support review, accountability and improvement decisions No additional teaching guidance is provided for this teaching content.
5.3 Impact of usability, accessibility and reliability
5.3.1 The impact of system performance, reliability and security issues on user experience, productivity and service continuity No additional teaching guidance is provided for this teaching content.

5.3.2 Principles of usability and accessibility and their relevance to system performance, reliability and security for diverse users could include:
 	
• examples of recognised accessibility standards:
  ○ WCAG
  ○ accessibility requirements set out under the Equality Act 2010
• examples of usability principles:
  ○ consistency, so the same action behaves the same way throughout
  ○ visibility of system status, so the user can see what is happening
  ○ error prevention and recovery, so mistakes are hard to make and easy to undo.
 	
Worked example of interface design affecting user effectiveness
Two versions of a sign-in screen ask users for the same details. The first clearly labels each field, provides instructions before entry and gives useful feedback when a sign-in attempt fails. The second relies on placeholder text that disappears when typing begins and provides only a generic error message. This gives users less support to identify and correct mistakes, particularly those using screen readers or who have difficulty remembering instructions. Repeated failed attempts may delay access or lead to an account being temporarily locked where a lockout control is in place.

5.3.3 The contribution of inclusive and accessible testing practices to reliable digital systems for diverse users No additional teaching guidance is provided for this teaching content.
5.3.4 Environmental and sustainability considerations associated with system performance and efficient use of digital resources No additional teaching guidance is provided for this teaching content.
5.4 Role of digital tools and AI-enabled testing

DRAFT

Teaching guidance
5.4.1 The role of contemporary digital tools in supporting test planning, identification of patterns in system behaviour and summarisation of findings No additional teaching guidance is provided for this teaching content.

5.4.2 The role of digital tools and automated and AI-enabled systems in supporting system configuration, testing and identification of patterns in system behaviour, and the need to review outputs to ensure accuracy and suitability could include:
 	
• examples of automated and AI-enabled support in testing:
  ○ automated test execution
  ○ pattern and anomaly detection in system behaviour
  ○ summarisation of test outputs
• examples of reasons for reviewing automated outputs before acting on them:
  ○ errors in an output may not be visible from the output itself
  ○ an output may be acted on by others who assume it has already been checked
• examples of checks supporting the accuracy and suitability of automated outputs:
  ○ ensuring data is valid before it is input
  ○ reviewing the prompts and information supplied to the system
  ○ comparing the output against the source it was produced from.
 	
Worked example of checking an automated summary
An automated tool summarises a test run as ‘all critical tests passed’. Comparing the summary with the underlying results shows that one critical test was skipped, but the summary incorrectly reported it as passed. Relying on the summary alone could lead to a system being signed off without all critical tests having been completed.

5.5 Principles of secure and responsible operation
5.5.1 Policies relating to data protection, privacy and acceptable system use, and their role in guiding configuration practice No additional teaching guidance is provided for this teaching content.
5.6 Configure and test digital systems to confirm readiness for use
5.6.1 Interpret user and system requirements to determine configuration needs and the scope and focus of testing No additional teaching guidance is provided for this teaching content.
5.6.2 Prepare and configure digital systems to meet defined needs No additional teaching guidance is provided for this teaching content.
5.6.3 Adjust configuration settings relating to user access, connectivity, storage and security to support system functionality and accessibility No additional teaching guidance is provided for this teaching content.
5.6.4 Carry out structured tests to confirm system functionality, performance, stability and security-related behaviours could include:

DRAFT

Teaching guidance

• examples of tests for each behaviour:
  ○ functionality, such as checking that valid credentials allow a user to sign in and incorrect credentials are rejected
  ○ performance, such as measuring system response times when multiple users access the system simultaneously
  ○ stability, such as checking that the system continues to operate without failure over an extended period
  ○ security-related behaviour, such as confirming that an account locks after repeated failed sign-ins where this is a defined requirement.
 	
Worked example of a structured test
A test record specifies that a user entering valid credentials should be signed in and taken to their own account page. The tester enters the username and correct password, selects 'Sign in' and compares the actual outcome with the expected result. The test passes if the correct account page opens and fails if the login is rejected, access to the wrong account is granted or an unexpected error occurs.

5.6.5 Assess system usability and accessibility against stated user needs No additional teaching guidance is provided for this teaching content.
5.6.6 Review system behaviour and outputs to identify deviations from expected outcomes and apply structured fault-finding approaches where required No additional teaching guidance is provided for this teaching content.
5.6.7 Record and compare test outcomes against requirements using accurate terminology and structured formats No additional teaching guidance is provided for this teaching content.
5.6.8 Evaluate test outcomes in relation to defined requirements to determine whether systems are ready for use or require further adjustment No additional teaching guidance is provided for this teaching content.
5.6.9 Identify and correct configuration settings related to user access, connectivity, storage and security that do not meet defined user requirements No additional teaching guidance is provided for this teaching content.
5.6.10 Apply routine checks to confirm systems are ready for use: user access and authentication, connectivity and network access, storage availability, software updates and security settings, expected system functionality and performance No additional teaching guidance is provided for this teaching content.
5.6.11 Apply policies relating to configuration and data protection requirements: secure configuration, access permissions, protection of personal information and software updates No additional teaching guidance is provided for this teaching content.
5.6.12 Document configuration decisions clearly No additional teaching guidance is provided for this teaching content.

DRAFT

Teaching guidance
5.6.13 Communicate configuration outcomes clearly and respond to queries in line with workplace procedures No additional teaching guidance is provided for this teaching content.
5.6.14 Maintain system integrity through responsible configuration practices, updates, permissions and security settings No additional teaching guidance is provided for this teaching content.

Transferable skills

The following transferable skills have been integrated into the content for work-related purposes:

- **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.

Workplace behaviours

Teaching and learning opportunities to develop the following workplace behaviours may be developed through learner engagement with this theme:

- **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 others, particularly when handling technical issues or responding to queries
- **responsive** when addressing system issues, user needs or emerging risks, including appropriate escalation where required.

DRAFT

Theme 6 Digital solution design and development

Theme summary			
The aim of this theme is to develop the knowledge, understanding and skills required to analyse user needs and design and create structured digital solutions that meet defined requirements, constraints and governance expectations. Solutions may include configurable, scripted, automated or low-code approaches. Learners are not required to use a specific technology, platform or programming language.			
Assessment			
Non-exam assessment (NEA)			
Optional Where this optional theme is selected, the teaching content and mandatory additional information must be covered by the tutor during the delivery of this qualification.	**Assessment reference** Refer to the scheme of assessment in Section 1.	**Level 3**	**80 GLH** Refer to the scheme of assessment in Section 1 for NEA assessment durations.

6.1 Approaches to problem analysis and requirements

Teaching content The learner must know and understand	**Mandatory additional information**
6.1.1 The purpose of analysing user needs and requirements when designing digital solutions	N/A

6.1.2 Approaches used to define problems, determine solution scope and identify constraints	• 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
	• techniques for defining a problem:
	  ○ stakeholder analysis
	  ○ SWOT analysis

6.1.3 How digital systems, components and processes influence the feasibility and structure of proposed solutions	• trade-offs between functionality, complexity and maintainability
	• further factors in feasibility trade-offs:
	  ○ cost
	  ○ security
	  ○ scalability
	  ○ accessibility
	  ○ time management

DRAFT

Teaching content The learner must know and understand	Mandatory additional information
6.1.4 The role of requirements, assumptions and success criteria in shaping solution proposals	• validation of assumptions and their impact on solution effectiveness
6.1.5 The relationship between user needs, workplace context and effective digital solution design	N/A

6.2 Principles of logic, algorithms and solution development

Teaching content The learner must know and understand	Mandatory additional information
6.2.1 The role of structured logic and step-by-step processes in designing digital solutions to define how inputs, processes and outputs are organised	• the relationship between logic structure and predictability of outcomes
6.2.2 Principles of algorithms, and structured coding approaches used to represent, sequence and control solution logic within digital designs	N/A

6.2.3 The purpose and characteristics of low-code and block-based development approaches	• how they support rapid prototyping, iterative design and early-stage exploration of digital solution ideas
	• benefits of low-code and block-based approaches:
	  ○ reduced barrier to entry
	  ○ faster stakeholder feedback

6.2.4 Principles, concepts and approaches underpinning digital design and structured logic in low-code and block-based environments	• abstraction, decomposition, sequencing, selection and iteration • how these support the development of reliable and maintainable digital solutions
6.2.5 The contribution of structured problem solving and logical thinking to robust solution proposals	N/A

DRAFT

6.3 Principles of user experience and design refinement

Teaching content The learner must know and understand	Mandatory additional information
6.3.1 Principles of user experience and user interface design that support usability and accessibility	• the relationship between interface design and user behaviour
6.3.2 The purpose of low-fidelity representations in communicating solution ideas during early stages of design	N/A
6.3.3 How design decisions influence usability, accessibility and system behaviour in digital solutions	N/A
6.3.4 The role of analysis and planning in reducing risk during later stages of development	N/A
6.3.5 The role of documentation and shared understanding in enabling development decisions	N/A

6.4 Role and implications of automated and AI-enabled design

Teaching content The learner must know and understand	Mandatory additional information

6.4.1 The role of automated and AI-enabled systems in supporting solution design, and the need to assess the suitability and limitations of outputs	• generating, refining and evaluating solution approaches
	• further uses of automated and AI-enabled systems in design:
	  ○ summarising requirements
	  ○ generating test cases
	  ○ producing documentation drafts

6.4.2 Governance requirements relevant to digital solutions that use automated and AI-enabled systems	N/A

6.4.3 Potential risks associated with automated decision-making in digital systems and their implications for users and organisations	• limitations of automated decision-making
	• the need for human oversight
	• further risks of automated decision-making:
	  ○ automation bias
	  ○ feedback loops that reinforce earlier outputs
	• safeguards alongside human oversight:
	  ○ how an automated decision was reached (explainability)
	  ○ when an automated decision can be challenged or overturned (contestability)

DRAFT

6.4.4 The implications of incorporating automated and AI-enabled processes into digital solutions	N/A

6.5 Considerations in responsible and governed solution design

Teaching content The learner must know and understand	**Mandatory additional information**
6.5.1 Policies and procedures relating to accessibility, data protection, security and responsible design and their influence on solution proposals	• designing for accessibility and diverse user needs • protection and appropriate use of personal and sensitive information • secure authentication and access control • responsible and ethical use of automated and AI-enabled systems
6.5.2 The importance of aligning proposed solutions with workplace policies and operational constraints relating to data protection, security, accessibility and acceptable system use	• protection and appropriate use of personal and sensitive information • secure authentication and access control • accessibility and the needs of diverse users • acceptable use of systems, devices and services • technical, organisational and resource constraints that affect solution feasibility and implementation
6.5.3 The importance of oversight, accountability and transparency in digital solution design	N/A
6.5.4 Sustainability considerations in digital solution design	• efficient use of resources • energy consumption • device lifecycle

6.6 Design and represent a digital solution to meet defined user needs

Teaching content The learner must be able to	**Mandatory additional information**
6.6.1 Interpret defined user needs and requirements to inform solution design	N/A
6.6.2 Analyse a problem to identify inputs, outputs, constraints and success criteria	N/A
6.6.3 Structure a proposed digital solution using logical steps and processes	N/A
6.6.4 Design solution concepts that consider system behaviour, user interaction and accessibility	N/A
6.6.5 Produce a clear and structured solution proposal suitable for development	N/A

DRAFT

Teaching content The learner must be able to	**Mandatory additional information**
6.6.6 Use appropriate development tools, environments and structured inputs (for example, prompts for automated and AI-enabled systems) to create, refine or represent a digital solution in line with defined requirements	N/A
6.6.7 Represent solution ideas using specified technical formats (for example, documents, presentations, spreadsheets, databases)	N/A
6.6.8 Justify design decisions in relation to user needs, requirements and governance considerations	N/A
6.6.9 Document assumptions, decisions and constraints clearly and accurately	N/A
6.6.10 Communicate proposed solutions clearly to technical and non-technical audiences	N/A

Teaching guidance
This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive.
6.1 Approaches to problem analysis and requirements
6.1.1 The purpose of analysing user needs and requirements when designing digital solutions No additional teaching guidance is provided for this teaching content.
6.1.2 Approaches used to define problems, determine solution scope and identify constraints No additional teaching guidance is provided for this teaching content.
6.1.3 How digital systems, components and processes influence the feasibility and structure of proposed solutions No additional teaching guidance is provided for this teaching content.

6.1.4 The role of requirements, assumptions and success criteria in shaping solution proposals could include:
 	
• examples of exploring and checking assumptions early:
  ○ asking the people affected directly, by phone call, interview, survey or site visit
  ○ prototyping, to test whether an approach works before committing to it
  ○ pilot testing with a small group before wider rollout
  ○ A/B testing, comparing two versions to see which performs better
  ○ using an AI tool to explore possibilities before checking them against real conditions.

6.1.5 The relationship between user needs, workplace context and effective digital solution design

DRAFT

Teaching guidance
No additional teaching guidance is provided for this teaching content.
6.2 Principles of logic, algorithms and solution development

6.2.1 The role of structured logic and step-by-step processes in designing digital solutions to define how inputs, processes and outputs are organised could include:
 	
• examples of how changing the sequence of steps changes the output:
  ○ calculating an order total by applying a discount before or after adding a fixed delivery charge, where the stated rule requires discounting the goods only
  ○ transforming data before building the chart or dashboard rather than after.

6.2.2 Principles of algorithms, and structured coding approaches used to represent, sequence and control solution logic within digital designs No additional teaching guidance is provided for this teaching content.

6.2.3 The purpose and characteristics of low-code and block-based development approaches could include:
 	
• examples of how the two approaches differ:
  ○ low-code, which uses pre-built components so a solution can be produced without building from scratch and without extensive programming experience
  ○ block-based, which removes the need to write syntax and is used mainly to develop and demonstrate logic
• examples of where each benefit applies:
  ○ reduced barrier to entry, which applies most strongly to block-based approaches
  ○ faster stakeholder feedback, which applies most strongly to low-code approaches
• examples of limitations of low-code and block-based approaches:
  ○ scaling ceilings, where an approach suited to early-stage prototyping stops being viable at scale
  ○ high-performance requirements that the approaches cannot meet.

6.2.4 Principles, concepts and approaches underpinning digital design and structured logic in low-code and block-based environments No additional teaching guidance is provided for this teaching content.
6.2.5 The contribution of structured problem solving and logical thinking to robust solution proposals No additional teaching guidance is provided for this teaching content.
6.3 Principles of user experience and design refinement

6.3.1 Principles of user experience and user interface design that support usability and accessibility could include:
 	
• examples of design choices that change user behaviour:
  ○ default settings, where an option is pre-selected and the user has to act to change it
  ○ layout and visual hierarchy, including what is made prominent and what appears first
  ○ gamification, including points and badges
  ○ user-centred design, where the design is built around what the user needs to do.

DRAFT

Teaching guidance

6.3.2 The purpose of low-fidelity representations in communicating solution ideas during early stages of design could include:
 	
• examples of low-fidelity representations:
  ○ sketches on paper
  ○ wireframes showing layout without detail
  ○ flow diagrams showing the steps a user takes.
 	
Worked example of low-fidelity representations in use
Two rough sketches of a booking screen are quickly produced on paper and shown to users before development begins. One asks for a date first, the other for the service. Users find the first confusing because they need to choose a service before selecting a date. The sketches are inexpensive to produce and easy to change, allowing the design to be revised before time and resources are committed to development.

6.3.3 How design decisions influence usability, accessibility and system behaviour in digital solutions No additional teaching guidance is provided for this teaching content.
6.3.4 The role of analysis and planning in reducing risk during later stages of development No additional teaching guidance is provided for this teaching content.
6.3.5 The role of documentation and shared understanding in enabling development decisions No additional teaching guidance is provided for this teaching content.
6.4 Role and implications of automated and AI-enabled design
6.4.1 The role of automated and AI-enabled systems in supporting solution design, and the need to assess the suitability and limitations of outputs No additional teaching guidance is provided for this teaching content.
6.4.2 Governance requirements relevant to digital solutions that use automated and AI-enabled systems No additional teaching guidance is provided for this teaching content.

6.4.3 Potential risks associated with automated decision-making in digital systems and their implications for users and organisations could include:
 	
• examples of automated decisions affecting people:
  ○ an account flagged as fraudulent and blocked without the cause being checked
  ○ a recruitment tool ranking candidates, where only those ranked highest are reviewed.
 	
Worked example of an automated decision given without explanation
An online system rejects a customer's loan application without explanation. The customer cannot tell whether the decision was based on incorrect or incomplete information, making it difficult to challenge. Staff also lack the information needed to review or reconsider the decision because they cannot identify which information or criteria led to the rejection.

6.4.4 The implications of incorporating automated and AI-enabled processes into digital solutions

DRAFT

Teaching guidance
No additional teaching guidance is provided for this teaching content.
6.5 Considerations in responsible and governed solution design
6.5.1 Policies and procedures relating to accessibility, data protection, security and responsible design and their influence on solution proposals No additional teaching guidance is provided for this teaching content.
6.5.2 The importance of aligning proposed solutions with workplace policies and operational constraints relating to data protection, security, accessibility and acceptable system use No additional teaching guidance is provided for this teaching content.
6.5.3 The importance of oversight, accountability and transparency in digital solution design No additional teaching guidance is provided for this teaching content.
6.5.4 Sustainability considerations in digital solution design No additional teaching guidance is provided for this teaching content.
6.6 Design and represent a digital solution to meet defined user needs
6.6.1 Interpret defined user needs and requirements to inform solution design No additional teaching guidance is provided for this teaching content.
6.6.2 Analyse a problem to identify inputs, outputs, constraints and success criteria No additional teaching guidance is provided for this teaching content.
6.6.3 Structure a proposed digital solution using logical steps and processes No additional teaching guidance is provided for this teaching content.
6.6.4 Design solution concepts that consider system behaviour, user interaction and accessibility No additional teaching guidance is provided for this teaching content.
6.6.5 Produce a clear and structured solution proposal suitable for development No additional teaching guidance is provided for this teaching content.
6.6.6 Use appropriate development tools, environments and structured inputs (for example, prompts for automated and AI-enabled systems) to create, refine or represent a digital solution in line with defined requirements No additional teaching guidance is provided for this teaching content.

6.6.7 Represent solution ideas using specified technical formats (for example, documents, presentations, spreadsheets, databases) could include:
 	
• examples of formats suited to different purposes:
  ○ a document with a labelled diagram, showing how the parts of a solution connect
  ○ presentation slides, taking an audience through an idea step by step

DRAFT

Teaching guidance
○ a spreadsheet showing the costs involved or the data that a solution will use ○ a database structure, showing what information a solution stores. **Worked example of one solution idea in two formats** A proposed booking system is represented as a labelled diagram within a document and as a sequence of presentation slides. The diagram shows how the parts connect at a glance and suits a technical reader; the slides take a non-technical audience through it one step at a time.
6.6.8 Justify design decisions in relation to user needs, requirements and governance considerations No additional teaching guidance is provided for this teaching content.
6.6.9 Document assumptions, decisions and constraints clearly and accurately No additional teaching guidance is provided for this teaching content.
6.6.10 Communicate proposed solutions clearly to technical and non-technical audiences No additional teaching guidance is provided for this teaching content.

Transferable skills

The following transferable skills have been integrated into the content for work-related purposes:

- **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.

Workplace behaviours

Teaching and learning opportunities to develop the following workplace behaviours may be developed through learner engagement with this theme:

- **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.

DRAFT

Section 3: key terms and definitions

Glossary of terms

This glossary provides the DfE definitions of subject terms relevant to this qualification.

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.
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.
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.
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.
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.

DRAFT

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.
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.
Lifecycle 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.
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.
Outcome	The result produced by an action, process or system.

DRAFT

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.
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.
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.
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.
Vulnerability	A weakness in a system, configuration, process or control that could be exploited to compromise security, functionality or reliability.

DRAFT

Digital technology abbreviations

This table lists the full terms for abbreviations used in the teaching content for this qualification.

CIA	Confidentiality, integrity and availability
IT	Information technology
MAC	Mandatory access control
MFA	Multi-factor authentication
NCSC	National Cyber Security Centre
PIN	Personal identification number
RACI	Responsible, accountable, consulted and informed
RBAC	Role-based access control
SWOT	Strengths, weaknesses, opportunities and threats
UK GDPR	UK General Data Protection Regulation
WCAG	Web Content Accessibility Guidelines

DRAFT

Section 4: support

Support materials

Support materials to assist with the delivery of this qualification are available on the qualification page on the NCFE website.

Other support materials

The resources and materials used in the delivery of this qualification must be age-appropriate and due consideration should be given to the wellbeing and safeguarding of learners in line with your institute's safeguarding policy when developing or selecting delivery materials.

Reproduction of this document

Reproduction by approved centres is permissible for internal use under the following conditions:

- you may copy and paste any material from this document; however, we do not accept any liability for any incomplete or inaccurate copying and subsequent use of this information
- the use of PDF versions of our support materials on the NCFE website will ensure that correct and up-to-date information is provided to learners
- any photographs in this publication are either our exclusive property or used under licence from a third party:
- they are protected under copyright law and cannot be reproduced, copied or manipulated in any form
    - this includes the use of any image or part of an image in individual or group projects and assessment materials
    - all images have a signed model release.

DRAFT

Contact us

NCFE
Q6
Quorum Park
Benton Lane
Newcastle upon Tyne
NE12 8BT

Tel: 0191 239 8000*
Email: customersupport@ncfe.org.uk
Website: www.ncfe.org.uk

DRAFT

NCFE © Copyright 2026. All rights reserved worldwide.

DRAFT Version 1.0 October 2026
Information in this Qualification Specification is correct at the time of publishing but may be subject to change.

NCFE is a registered charity (Registered Charity No. 1034808) and a company limited by guarantee (Company No. 02896700).

CACHE; Council for Awards in Care, Health and Education; and NNEB and ACTIVE IQ are registered trademarks owned by NCFE.

All the material in this publication is protected by copyright.

To continue to improve our levels of customer service, telephone calls may be recorded for training and quality purposes.

Appendix A: themes

To simplify cross-referencing assessments and quality assurance, we have used a sequential numbering system in this document for each theme.

 Themes covering knowledge and understanding only are indicated by a star. All other themes cover skills or a mix of knowledge, understanding and skills.

Mandatory themes

	Theme number	Theme title	Level	GLH
☆	1	Principles of systems, configuration and fault resolution	3	60
	2	Data analytics and decision-making	3	80
☆	3	Principles of communication, problem solving and ethical practice	3	60
	4	Cyber security operations and response	3	80

Optional themes

Theme number	Theme title	Level	GLH
5	Digital systems configuration and assurance	3	80
6	Digital solution design and development	3	80

DRAFT

Change history record

Version	Publication date	Description of change

DRAFT