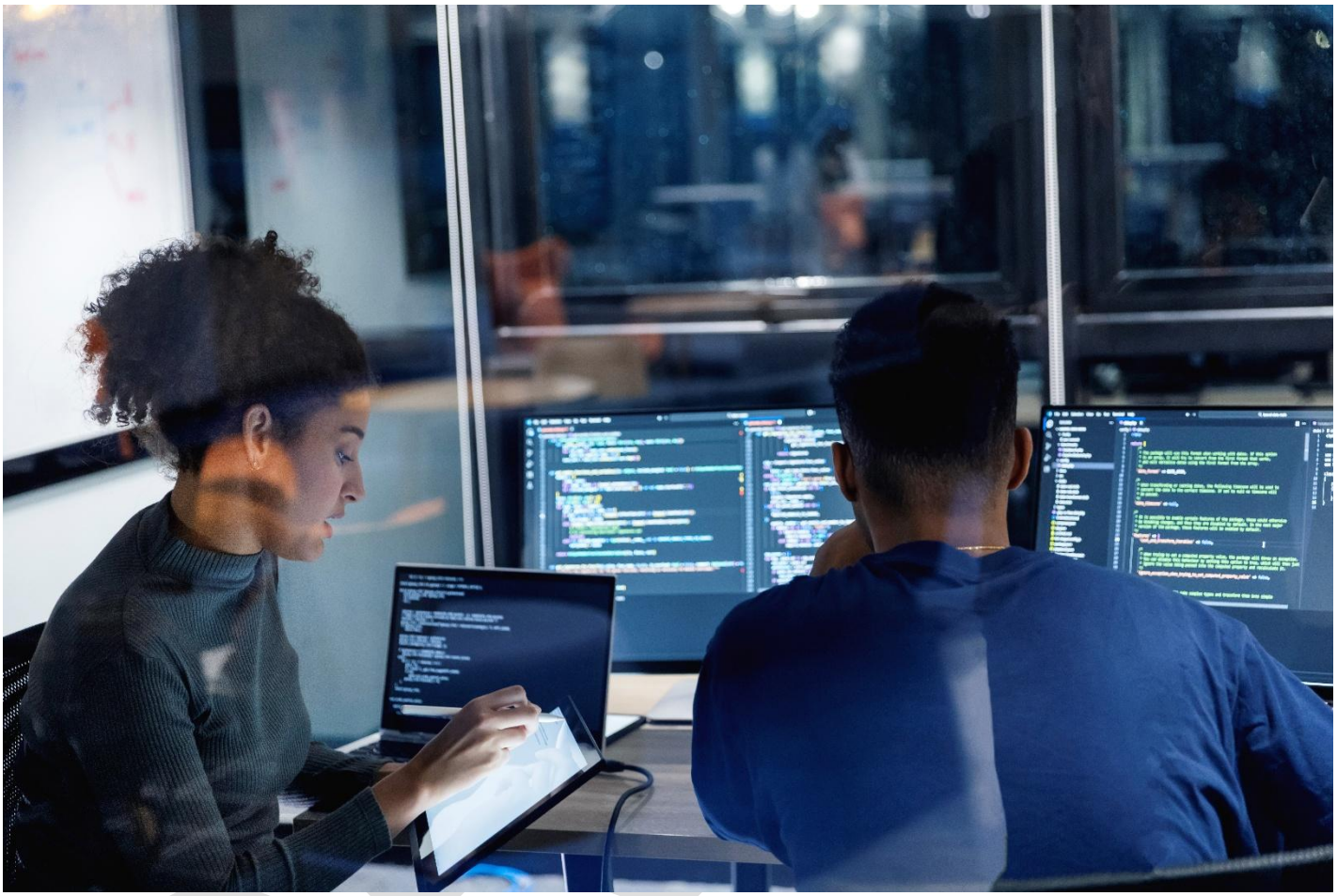
NCFE Level 2 Foundation Certificate in Digital Systems and Data

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 2 Foundation Certificate in Digital Systems and Data**
Ofqual qualification number (QN)	TBC
Guided learning hours (GLH)	300
Total qualification time (TQT)	375
Duration	1 year
Minimum age	16
Qualification aim	This qualification is designed for 16 to 19-year-olds who wish to build their confidence and develop foundational knowledge and skills in digital systems and data. It develops learners' knowledge, understanding and skills in relation to digital technology, and the ability to apply these to practical work-related activities, preparing them for progression to level 3 study in a related subject area, such as V Levels, T Levels or A levels.
Grading	Pass/merit/distinction/unclassified (P/M/D/U)
Assessment method	40% Assessment by examination (AbE) 60% Non-exam assessment (NEA)
Synoptic assessment	This qualification includes synoptic assessment across 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.
Performance points	Please check the performance points data produced by the Department for Education (DfE).
Funding	Foundation Certificates 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 2 Foundation Certificate subject content, July 2026.

DRAFT

Contents

Qualification summary **2**

Section 1: introduction **5**

Aims and objectives 5
Literacy, numeracy and digital skills 5
Key theories and principles 6
Guidance for entry and registration 7
Achieving this qualification 7
Progression 7
Staffing requirements 7
Resource requirements 8
Work/industry placement experience 8
How the qualification is assessed 8
Non-exam assessment (NEA) 9
Assessment by examination (AbE) 9
Controlled external quality assurance 9
Enquiries about results 10
Unclassified grade 11
External assessment conditions 11
Resubmission of non-exam assessments (NEAs) 11
Retakes of assessment by examination (AbE) 11
Refresh of assessments 11
Scheme of assessment 12
Assessment objectives (AOs) 13
Assessment objective (AO) weightings 13
Grading information 13
Requirements for referencing 14
Group and collaborative working 14
Plagiarism and use of artificial intelligence (AI) 15
Guidance on delivering sensitive content 15
Access arrangements, reasonable adjustments and paper modifications 16

Section 2: themes and assessment guidance **17**

Delivery guidance 17
Theme 1: Preparing and visualising data 18
Theme 2: System configuration and security 22
Theme 3: Plan, develop and test a programming solution 27
Theme 4: Plan and configure hardware and software 31
Theme 5: Digital research and evidence-based recommendations 34

Section 3: key terms and definitions **38**

Glossary of terms 38
Digital technology abbreviations 40

Section 4: support **42**

Support materials 42
Other support materials 42
Reproduction of this document 42

Contact us **43**

DRAFT

Appendix A: themes **44**

Mandatory themes 44

Change history record **45**

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 Foundation Certificate is a level 2 vocational qualification, aimed at preparing learners for progression to level 3 study through applied, work-related learning. This qualification's specific size reflects the teaching and learning required for the subject. It forms part of a wider study programme, which may also include English and maths where required.

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:

- provide learners with nationally agreed knowledge, understanding and skills in relation to digital technology
- develop learners' ability to apply knowledge, understanding and skills to practical work-related activities
- build learners' confidence and readiness to progress to level 3 study, such as V Levels, T Levels or A levels.

The objectives of this qualification are:

- prepare, analyse, interpret and visualise data, apply security practices to configure and protect digital systems, and communicate findings effectively
- apply core digital knowledge and skills to design, develop and test digital solutions while developing problem-solving, communication and responsible digital practice.

Literacy, numeracy and digital skills

Learners must continue to develop literacy, numeracy and digital skills through applying them in the context of the themes in Section 2. These skills are developed through delivery of the mandatory teaching content and are not assessed separately.

Literacy

Learners will develop literacy skills, including:

- reading and interpreting technical information, briefs, datasets and digital documentation
- using subject-specific and technical vocabulary accurately
- recording processes, decisions and findings clearly in structured formats
- summarising information, drawing conclusions and explaining reasoning
- communicating findings, risks and recommendations clearly for different audiences
- acknowledging and referencing digital sources appropriately.

DRAFT

Numeracy

Learners will develop numeracy skills, including:

- interpreting numerical data, including totals, averages and proportions
- identifying patterns, trends and anomalies within datasets
- checking accuracy and consistency of numerical information
- applying numerical reasoning to support conclusions, risk identification and troubleshooting
- using quantitative evidence to justify recommendations and decisions.

Digital

Learners will develop digital skills, including:

- using digital tools and applications to clean, interpret, visualise and present data
- configuring hardware, software and network components securely
- developing, testing and refining programming solutions
- managing digital information by producing, organising, storing and retrieving content.

Key theories and principles

Learners will develop knowledge and understanding of the key theories and principles that support effective practice in the subject, including:

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

The aspects listed above are indicative of the scope and intent of the qualification and are not intended to be exhaustive.

DRAFT

Guidance for entry and registration

This qualification is designed for learners aged 16 to 19 who wish to develop their knowledge, understanding and skills in digital systems and data.

It may also be useful to learners studying qualifications in the following sectors/areas:

- computer science
- digital
- information technology.

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 1 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 this qualification and complying with the relevant literacy, numeracy, and health and safety requirements.

Learners registered on this qualification should not undertake another qualification at the same level, or with the same/a similar title, as duplication of learning may affect funding eligibility.

Achieving this qualification

To be awarded this qualification, learners must complete the required teaching content within the mandatory themes, undertake all required assessments and meet the qualification's grading requirements.

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

Progression

Learners who achieve this qualification could progress to the following:

- further education:
  - V Levels (Level 3 V Level in Digital Systems and Data)
  - T Levels (Digital Software Development, Digital Support and Security and Digital Data Analytics)
  - A levels (Computer Science)
  - appropriate apprenticeship progression at level 2 or level 3.

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
- have a sufficient number of appropriately qualified/experienced internal quality assurers (IQAs) to internally quality assure the anticipated number of assessors and learners

DRAFT

- 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

To assist in the delivery of this qualification, centres/learners should have access to the following mandatory resources:

- computers/laptops
- internet access.

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 skill, knowledge and understanding against the standards set in a qualification.

This qualification uses a combination of centre-marked assessment, controlled external quality assurance and external assessment.

The assessments for this qualification are synoptic, which allows 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 – which 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 controlled external quality assurance must be in English.

Non-exam assessment (NEA)

The NEA within this qualification is externally set and centre marked, with NCFE completing controlled external quality assurance. Centres are not permitted to adapt NEA tasks.

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

The NEA encourages 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 NEA must be supervised and assessed by the tutor. The NEA 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 NEA are available on the NCFE website.

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: Preparing and visualising data
- Theme 2: System configuration and security
- Theme 3: Plan, develop and test a programming solution
- Theme 4: Plan and configure hardware and software
- Theme 5: Digital research and evidence-based recommendations.

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.

Controlled external quality assurance

DRAFT

This qualification is subject to a controlled external quality assurance model, providing enhanced oversight and scrutiny. All centres will be subject to a structured external review of assessment and internal quality assurance decisions using standardised sampling, ensuring that all results are reviewed and confirmed prior to their release.

Centres must submit final grades for each NEA by the published deadline and upload the requested learner evidence and assessment records for the selected sample through NCFE systems. Any actions identified through the external quality assurance process must be addressed before results are confirmed, where required. Ongoing monitoring will also be undertaken to identify and address any emerging risks to assessment validity and consistency.

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.

DRAFT

Unclassified grade

Learners who do not achieve a pass will receive an unclassified (U) result.

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.

Resubmission of non-exam assessments (NEAs)

Learners will have one resubmission opportunity for the NEA. The resubmission could be used to:

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

Feedback to learners can only be given to clarify areas where they have not achieved a minimum or expected level of performance. Learners cannot receive any guidance on how to improve their work to achieve a higher mark or grade. It is the centre's responsibility to keep the evidence of the learner's original and revised work submitted, and records of the initial grade, assessor feedback, and final grade, for controlled external quality assurance purposes.

If a learner fails to meet the pass criteria following the resubmission with revised evidence, there is no opportunity for a retake and no results are carried forward.

Retakes of assessment by examination (AbE)

AbE is available in Series 1. There are no retake opportunities for the AbE.

Refresh of assessments

To reduce predictability and maintain assessment integrity, assessment scenarios will vary between series and will be set within a range of realistic digital systems and data contexts, ensuring that assessments cannot be anticipated.

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	Delivery mode	Assessment weightings	Raw marks	UMS	Assessment conditions	Marking
AbE	1.5 hours	Mandatory	Paper-based or on screen	40%	60	80	Invigilated	Externally marked
NEA	14.5 hours	Mandatory	Paper-based or on screen	60%	N/A	120	Supervised	Centre marked and controlled external quality assurance
Assessment total	16 hours			100%	60	200		

DRAFT

Assessment objectives (AOs)

The following table outlines the AOs for this qualification and defines each one.

AOs	Definition
AO1	Demonstrate knowledge and understanding of concepts, processes and principles in digital systems and data.
AO2	Apply knowledge and understanding of key requirements and approaches in digital systems and data to different situations and contexts.

Assessment objective (AO) weightings

The following table shows the weighting allocated to each AO within the assessment.

AOs	Weighting (%)
AO1	20%
AO2	80%

Grading information

Assessment of this qualification is graded as pass, merit and distinction. Learners who do not achieve a pass will receive an unclassified (U) result.

Uniform mark scale (UMS) scores are used to standardise performance across assessments. For each assessment, only the highest UMS score from any repeated attempts is used, and high performance in one area can compensate for lower performance in another.

This compensatory approach, combined with the use of a UMS, means that the boundaries for individual assessments do not directly add up to the overall qualification boundaries. This allows learners to balance weaker performance in one area with stronger performance in another. For instance, a high score in the AbE can offset lower scores in the NEA.

The overall grade issued to a learner for the Foundation Certificate will be based on the aggregation of UMS points for each of the two assessment components and the overall UMS grade boundaries, which are set at fixed percentages of the maximum UMS.

The maximum UMS points available for each assessment and the qualification, as well as the UMS points relating to each grade boundary, will be fixed according to the table below:

The table below shows the grade boundaries for each assessment.

Grade boundary	AbE		NEA		Overall	
	%	UMS	%	UMS	%	UMS
Max	100	80			100	200
Distinction	80	64	90	108	80	160

Merit	60	48	70	84	60	120
Pass	40	32	50	60	40	80

The table below shows the overall qualification grade boundaries.

Grade boundary	UMS points
Pass	80
Merit	120
Distinction	160

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

NCFE does not anticipate any changes to our aggregation methods or any overall grade thresholds; however, there may be exceptional circumstances in which it is necessary to do so to secure the maintenance of standards over time. Therefore, overall grade thresholds published within this Qualification Specification may be subject to change.

Requirements for referencing

Carefully selected quotations must be included to support learners' own responses within the NEA. 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.

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.

DRAFT

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 account of 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 Joint Council for Qualifications (JCQ) published guidance.

Guidance on delivering sensitive content

When learners engage with sensitive topics, for example safeguarding, 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.

DRAFT

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 the grading scale, and guided learning hours (GLH), mandatory teaching content and teaching guidance.

Information in the teaching content section 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.

Delivery guidance

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

DRAFT

Theme 1: Preparing and visualising data

Theme summary		
This theme introduces learners to the common practice of working with a range of data types using structured datasets. Learners will learn to clean, interpret and visualise data for a defined purpose and then communicate findings, developing an understanding of how data is used to inform decisions within a digital context.		
Assessment		
Assessment by examination (AbE) and non-exam assessment (NEA).		
Mandatory Teaching content must be covered by the tutor during the delivery of this qualification.	**Level 2**	**60 GLH**

Subject topic	Teaching content The learner must know and understand:
1.1 Understand digital data	1.1.1 Numerical, text, categorical and date or time data types
	1.1.2 Digital data sources comprising spreadsheets, databases, survey outputs, online data repositories and system-generated reports
	1.1.3 The role of database structures and fields used to organise and retrieve structured data
	1.1.4 The role of emerging digital technologies in shaping digital systems and services
1.2 Data cleansing and preparation	1.2.1 The effect of missing values, duplicate records, inconsistent formatting and incorrect data types on accuracy and interpretation
	1.2.2 The efficient use, storage and handling of data to support responsible and sustainable digital practices
1.3 Visualising and communicating findings	1.3.1 The role of graphical and tabular formats, including their use within infographics, in supporting interpretation and communication of findings
	1.3.2 The role of spreadsheet and data presentation tools, and automated and AI-enabled features in supporting interpretation and presentation of data
	1.3.3 The contribution of clear written and visual communication when presenting findings

Subject topic	Teaching content The learner must be able to:
1.4 Data cleansing and preparation	1.4.1 Review datasets for accuracy and resolve missing values, duplicate records, inconsistent formatting and incorrect data types
	1.4.2 Format, clean and prepare digital datasets using spreadsheet and data presentation tools
1.5 Visualising and communicating findings	1.5.1 Create tables and charts to represent data
	1.5.2 Identify patterns and draw conclusions
	1.5.3 Communicate findings clearly for an intended purpose

DRAFT

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

1.1.1 Numerical, text, categorical and date or time data types:
 	
• uses for each data type may include:
  ○ numerical (for example, integer, decimal, percentage, currency)
  ○ text (for example, string, free text, email address)
  ○ categorical (for example, Boolean, binary, nominal, ordinal)
  ○ date or time (for example, date, time, timestamp, duration).

1.1.3 The role of database structures and fields used to organise and retrieve structured data:
 	
• roles of database structure:
  ○ organise data (for example, tables, rows, columns)
  ○ reduce duplication (for example, avoids repeatedly storing the same data)
  ○ relationships between data (for example, using keys to connect related data)
  ○ maintain accuracy (for example, validation and verification to prevent incorrect data input)
  ○ security (for example, controlling access to view or modify data)
  ○ maintenance (for example, a well-designed structure makes it easier to add, change, or remove information)
• retrieval, finding and getting specific information stored in a database when it is needed (for example, indexing).

1.2 Data cleansing and preparation

1.2.2 The efficient use, storage and handling of data to support responsible and sustainable digital practices:
 	
• working examples may include:
  ○ efficient use (only collecting data that is required)
  ○ storage (data organised so that it can be easily accessed, it is backed up and stored securely)
  ○ handling (protecting from loss or unauthorised access)
  ○ responsible practices (data protection and privacy requirements)
  ○ sustainable practices (deleting data no longer required to avoid excessive storage to reduce energy and resource use).

1.3 Visualising and communicating findings

1.3.1 The role of graphical and tabular formats, including their use within infographics, in supporting interpretation and communication of findings:
 	
• the role of graphical and tabular formats:
  ○ to present data visually using charts, graphs and tables
• purpose of infographics:
  ○ combine charts, graphs and tables to show data clearly and make it easier to understand and interpret
• supporting interpretation:
  ○ to help people understand the data (for example, identifying patterns and trends)
• communication of findings:
  ○ communicating the results clearly to allow people to understand any findings identified from the data.

1.3.2 The role of spreadsheet and data presentation tools, and automated and AI-enabled features in supporting interpretation and presentation of data:

DRAFT

Teaching guidance

• spreadsheets:
  ○ used to organise, clean, calculate and analyse data (for example, Excel or Google Sheets)
• data presentation tools:
  ○ used to turn data into dashboards and visual reports (for example, Power Bi or Tableau)
• automated features:
  ○ for example, automatically identifying duplicates or creating charts
• AI-enabled features:
  ○ AI tools that can help to identify patterns, recommend visualisation style or summarise data findings.

DRAFT

Transferable skills

Transferable skills to be demonstrated through this theme:

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

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

- planning:
  - structured activities such as cleaning datasets, developing code, configuring systems and delivering digital systems by identifying steps, sequencing tasks, estimating resources and managing time
- data interpretation:
  - data, systems and digital scenarios by organising information into types, identifying patterns and anomalies, deconstructing problems, and understanding how components interact
- communicating:
  - findings, risks and recommendations clearly using written, visual and digital formats, adapting explanations and terminology to suit purpose and audience
- investigating:
  - suitable digital sources, interrogating datasets, reviewing logs and dashboards, and designing and carrying out tests to confirm accuracy, function or security
- recording:
  - information accurately by capturing, storing and organising digital content such as datasets, code, configurations, findings and documentation.

Work-related behaviours

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

- attention to detail
- persistent
- reliable.

DRAFT

Theme 2: System configuration and security

Theme summary
This theme introduces learners to the practice of configuring and securing digital systems. By working with digital systems and network components, learners will configure digital systems, apply security measures and control, use log files and dashboards to monitor and review system information, identify security weaknesses and risks, and respond appropriately with consideration of confidentiality, integrity and availability (CIA) of data and services.
Assessment
Assessment by examination (AbE) and non-exam assessment (NEA).

Mandatory Teaching content must be covered by the tutor during the delivery of this qualification.	**Level 2**	**60 GLH**

Subject topic	Teaching content The learner must know and understand:
2.1 Introducing networks and system configurations	2.1.1 The operation of digital networks through connected devices, infrastructure components and software governed by communication protocols
	2.1.2 Communication between devices and connected systems within digital networks
	2.1.3 Communication protocols, IP addressing conventions, secure configuration baselines and patch management practices in supporting secure and reliable digital systems
	2.1.4 Health, safety and secure handling requirements when setting up, configuring or maintaining digital systems and equipment
2.2 System security	2.2.1 The meaning of confidentiality, integrity and availability in relation to protecting data, systems and services
	2.2.2 The causes and indicators of security weaknesses and risks arising from insecure access, weak authentication methods, unpatched software and misconfigured system or network settings
	2.2.3 Authentication measures, access permissions, configuration settings and protective controls in securing digital systems
2.3 Monitoring and incident management	2.3.1 The role of workplace policies and procedures in supporting secure system use and incident management: • acceptable use policies • access control and authentication requirements • incident reporting and escalation procedures • data protection requirements • privacy and confidentiality requirements
	2.3.2 The use of monitoring information, log files, dashboards and automated security tools in identifying potential weaknesses and supporting system security
	2.3.3 The role of digital tools, automated security scanning tools and AI-enabled systems in supporting secure configuration and identifying potential vulnerabilities, and the need to interpret, review and validate outputs before use

DRAFT

Subject topic	Teaching content The learner must be able to:
2.4 Introducing networks and system configurations	2.4.1 Configure digital systems by applying secure configuration, authentication requirements, access controls, permissions and security settings and update procedures
2.5 System security	2.5.1 Identify security weaknesses within digital systems and explain their potential impact on the confidentiality, integrity and availability of systems, devices and data
	2.5.2 Apply or recommend appropriate actions that support security improvement, troubleshooting and protection of digital systems
2.6 Monitoring and incident management	2.6.1 Review log files, monitoring dashboards, system alerts and other security-related information to identify signs of unexpected or anomalous activity
	2.6.2 Record and organise security-related information clearly and accurately using appropriate digital tools
	2.6.3 Communicate security concerns, risks and recommended actions clearly for different audiences
	2.6.4 Escalate potential cyber security concerns using defined workplace procedures
	2.6.5 Handle security-related information in accordance with privacy, confidentiality and data protection requirements

Teaching guidance

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

2.1 Introducing networks and system configurations

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

- connected devices may include:
  - computers/laptops
  - smartphones/tablets
  - printers
  - smart devices
- infrastructure components may include:
  - router
  - switch
  - wireless access point (WAP)
  - server
- software may include:
  - operating system (for example, Windows, MacOS, Linux)
  - applications (for example, web browser, email client, productivity suite)
- working example:
  - digital networks connect devices through physical infrastructure, using software to manage communication and protocols to set rules for how data is transmitted and received.

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

- communication protocols may include:
  - TCP/IP
  - HTTP/HTTPS

DRAFT

Teaching guidance
○ DNS ○ DHCP • IP addressing conventions may include: ○ devices require an appropriate IP address ○ duplicate IP addresses should be avoided ○ static IP addresses used where appropriate (for example, server, printer) ○ DHCP automatically assigns address for client devices • secure configuration baselines may include: ○ strong password policy ○ use of firewall and anti-virus ○ disabling services that are not needed ○ encryption ○ approval of software ○ user permissions ○ email filtering • patch management practices may include: ○ identifying updates ○ accessing importance ○ if required test in a sandbox ○ install patch and test it is successful.
2.1.4 Health, safety and secure handling requirements when setting up, configuring or maintaining digital systems and equipment: • health and safety may include: ○ electrical checks (for example, checking cables and power supplies) ○ workstation assessments (for example, screens, desks, chairs) ○ safe working environments (for example, workplace trips and hazards) ○ manual handling (for example, lifting/moving servers and racking) ○ electrostatic discharge (ESD) protection (for example, anti-static mats) • secure handling requirements may include: ○ use of strong passwords ○ access controls ○ data backups ○ system updates ○ security software ○ asset management • working example of replacing a hard drive may include: ○ back up data on the drive ○ securely erase all data from the drive ○ shut down and disconnect device from power ○ use anti-static protection when removing/replacing the drive ○ restore drive from backup.
2.2 System Security
2.2.2 The causes and indicators of security weaknesses and risks arising from insecure access, weak authentication methods, unpatched software and misconfigured system or network settings: • causes of security weaknesses and risks may include: ○ legacy software/hardware ○ weak passwords ○ poor configuration ○ human error

DRAFT

Teaching guidance

- missing security controls
- incorrect user permissions
- incorrect access controls
- limited physical security.

2.2.3 Authentication measures, access permissions, configuration settings and protective controls in securing digital systems:

- authentication measures may include:
  - passwords
  - PIN
  - biometrics
  - multi-factor authentication (MFA)
- users should only have the access permissions needed to perform their role:
  - principle of least privilege
- configuration settings and protective controls:
  - firewall
  - anti-virus
  - encryption
  - intrusion protection/detection system
  - backup (for example, full, incremental, differential)
  - access control methods (for example, role-based access control (RBAC)).

2.3 Monitoring and incident management

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

- role may include:
  - digital tool to help staff configure, manage and monitor systems securely (for example, log analysis tools)
  - automated security scanning tool to check systems for weakness without requiring manual inspection (for example, open or unnecessary network services/ports)
  - AI-enabled systems to help identify patterns (for example, identifying unusual behaviour)
- reasons for interpretation and reviewing:
  - false positives
  - false negatives
  - prioritisation of security concerns.

Transferable skills

Transferable skills to be demonstrated through this theme:

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

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

DRAFT

Transferable skills

• problem solving:
  ○ evaluating information, data, systems behaviour and AI-enabled outputs by questioning accuracy, weighing the pros and cons, applying logical reasoning and reaching justified conclusions
• communicating:
  ○ findings, risks and recommendations clearly using written, visual and digital formats, adapting explanations and terminology to suit purpose and audience
• investigating:
  ○ suitable digital sources, interrogating datasets, reviewing logs and dashboards, and designing and carrying out tests to confirm accuracy, function or security
• recording:
  ○ information accurately by capturing, storing and organising digital content such as datasets, code, configurations, findings and documentation
• observing:
  ○ situational awareness by monitoring system outputs, data quality, error messages, logs and alerts to identify issues or abnormal behaviour.

Work-related behaviours
Teaching and learning opportunities to develop the following work-related behaviours may be developed through learner engagement with this theme: • attention to detail • perceptive • responsible.

DRAFT

Theme 3: Plan, develop and test a programming solution

Theme summary		
This theme introduces learners to the foundational practice of planning, designing and developing a programming solution. By working with defined problems and briefs, learners will plan, develop and test a solution, building an understanding of the effect that logic errors, syntax errors and incorrect conditions can have on a program's behaviour.		
Assessment		
Assessment by examination (AbE) and non-exam assessment (NEA).		
Mandatory Teaching content must be covered by the tutor during the delivery of this qualification.	**Level 2**	**60 GLH**

Subject topic	Teaching content The learner must know and understand:
3.1 Solution planning and design	3.1.1 The stages of programming solution development and their role in meeting an intended purpose
	3.1.2 The role of algorithms as ordered instructions that determine solution behaviour
	3.1.3 The relationship between algorithms, program code and solution outputs
	3.1.4 The role of structured logic and algorithms in the design of digital solutions
3.2 Solution development	3.2.1 The use of developer-written and externally sourced code within digital solutions and the need to comply with licensing requirements
	3.2.2 The role of automated and AI-enabled tools in generating code suggestions, and the need to review, test and understand these outputs before use
3.3 Testing and debugging	3.3.1 The effect of logic errors, syntax errors and incorrect conditions on program behaviour
	3.3.2 The role of testing approaches in confirming that programming behaves as expected

Subject topic	Teaching content The learner must be able to:
3.4 Solution planning and design	3.4.1 Plan a programming solution to meet a given brief
3.5 Solution development	3.5.1 Develop a programming solution by writing and integrating code
	3.5.2 Apply a logical, step-by-step approach when developing and refining code
3.6 Testing and debugging	3.6.1 Use appropriate software tools to run and test the code within a solution
	3.6.2 Test the solution to confirm it produces the expected outcome
	3.6.3 Identify and correct errors in code
	3.6.4 Communicate outcomes clearly using concise explanations and structured documentation

DRAFT

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

3.1.1 The stages of programming solution development and their role in meeting an intended purpose:
 	
• programming solution development is the process of designing, creating, testing and maintaining computer programs to solve problems or meet specific needs
• stages of programming solution development:
  ○ identify the problem
  ○ design
  ○ development
  ○ testing
  ○ debugging
  ○ implementation
  ○ maintenance
• the role of software development life cycle (SDLC):
  ○ provides a framework
  ○ helps ensure the solution meets user requirements.

3.1.3 The relationship between algorithms, program code and solution outputs:
 	
• relationship between algorithms, program code and solution outputs:
  ○ an algorithm is a step-by-step set of instructions for solving a problem or completing a task
  ○ program code is the algorithm written in a programming language (for example, Python)
  ○ output is the result produced when the program code is executed.

3.2 Solution development

3.2.1 The use of developer-written and externally sourced code within digital solutions and the need to comply with licensing requirements:
 	
• externally sourced code may include:
  ○ open-source libraries
  ○ frameworks
  ○ code repositories (for example, GitHub)
  ○ third party APIs
  ○ snippets
• licensing requirements may include:
  ○ giving credit to the original developer
  ○ including copyright or licence information
  ○ following requirements when modifying code
  ○ following requirements when distributing or sharing code
  ○ checking whether commercial use is permitted.

3.2.2 The role of automated and AI-enabled tools in generating code suggestions, and the need to review, test and understand these outputs before use:
 	
• the role of automation can help developers create code more quickly (for example, finding possible errors)
• the role of AI-enabled tools can generate code based on instructions written in normal language
• review and test may include checking for:
  ○ bugs
  ○ incorrect results

DRAFT

Teaching guidance
○ inefficient code ○ security concerns ○ outdated usage methods/techniques • understand outputs may include: ○ reviewing generated code because it may contain errors or bugs ○ generated code may introduce vulnerabilities (for example, weak authentication) ○ generated code is written according to agreed rules and guidelines ○ developers' responsibility for the code they use.
3.3 Testing and debugging
3.3.1 The effect of logic errors, syntax errors and incorrect conditions on program behaviour: • effects may include: ○ logic error – the program runs but produces the wrong result because the instructions are incorrect ○ syntax error – the program cannot run because the code does not follow the rules of the programming language ○ incorrect condition – the program makes the wrong decision because a condition has been written incorrectly.
3.3.2 The role of testing approaches in confirming that programming behaves as expected: • testing approaches may include: ○ invalid testing (checks that the program rejects data that should not be accepted) ○ functional testing (checks each function works correctly) ○ boundary testing (checks limits of acceptable data) ○ system testing (tests the program as a whole).
3.5 Solution development
3.5.2 Apply a logical, step-by-step approach when developing and refining code: • step-by-step approach involves: ○ breaking a programming problem into smaller, manageable stages ○ completing them in a logical order • iterative development: ○ creating a program in stages ○ testing each stage ○ identifying improvements ○ repeating the process until the program works as expected.
3.6 Testing and debugging
3.6.1 Use appropriate software tools to run and test the code within a solution: • software tools may include: ○ code editor/IDE ○ compiler ○ interpreter ○ debugging ○ testing ○ version control ○ AI coding tools.

DRAFT

Transferable skills

Transferable skills to be demonstrated through this theme:

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

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

- planning:
  - structured activities such as cleaning datasets, developing code, configuring systems and delivering digital systems by identifying steps, sequencing tasks, estimating resources and managing time
- problem solving:
  - evaluating information, data, systems behaviour and AI-enabled outputs by questioning accuracy, weighing the pros and cons, applying logical reasoning and reaching justified conclusions
- investigating:
  - suitable digital sources, interrogating datasets, reviewing logs and dashboards, and designing and carrying out tests to confirm accuracy, function or security
- self-managing:
  - own performance by working through multi-stage tasks, monitoring progress, checking accuracy, responding to feedback and refining outcomes through testing and review
- recording:
  - information accurately by capturing, storing and organising digital content such as datasets, code, configurations, findings and documentation.

Work-related behaviours

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

- focused
- adaptable
- persistent.

DRAFT

Theme 4: Plan and configure hardware and software

Theme summary		
This theme introduces learners to the practice of planning, configuring and maintaining digital systems. By working with hardware and software components, learners will plan, sequence tasks and configure systems to produce and deliver digital systems. Learners will develop an understanding of components' compatibility and system requirements in configuring a functional digital system.		
Assessment		
Assessment by examination (AbE) and non-exam assessment (NEA).		
Mandatory Teaching content must be covered by the tutor during the delivery of this qualification.	**Level 2**	**60 GLH**

Subject topic	Teaching content The learner must know and understand:
4.1 Digital system planning	4.1.1 The role of planning tasks, sequencing activities and allocating resources when delivering a digital system
	4.1.2 The role of user interface elements, accessibility and digital content in supporting the usability of a digital system
	4.1.3 The role of component compatibility and system requirements in configuring a functional digital system
	4.1.4 The influence of dependencies between components on overall system operation
	4.1.5 Factors that affect the energy use, resource efficiency and sustainability of digital systems and devices
4.2 System configuration	4.2.1 The interaction between hardware and software components in enabling system functionality
	4.2.2 The role of digital tools, automation features and automated AI-enabled systems in generating configuration and supporting system setup, and the need to check such outputs for suitability for the intended system
4.3 Routine maintenance and troubleshooting	4.3.1 The occurrence of faults during configuration and operation and the need for checking, diagnosis and corrective action
	4.3.2 The contribution of maintenance activities comprising updates, checks and troubleshooting to continued system performance and reliability

Subject topic	Teaching content The learner must be able to:
4.4 Digital system planning	4.4.1 Plan and sequence tasks and resources to support delivery of a digital system
4.5 System configuration	4.5.1 Configure hardware and software components to achieve a functional digital system
4.6 Routine maintenance and troubleshooting	4.6.1 Verify system operation by checking that components function together as intended
	4.6.2 Perform routine maintenance activities to support continued operation
	4.6.3 Record and communicate configuration and maintenance activity clearly to others

DRAFT

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

4.1.3 The role of component compatibility and system requirements in configuring a functional digital system:
 	
• role of component compatibility may include:
  ○ components' compatibility with the motherboard (for example, CPU, RAM)
  ○ peripheral compatibility (for example, drivers, connectivity)
  ○ operating system (for example, supports components and drivers)
• system requirements in configuring a functional digital system:
  ○ processor (for example, speed, type)
  ○ RAM (for example, type)
  ○ storage (for example, HDD, SSD)
  ○ graphic card (for example, GPU, monitor compatibility)
  ○ network requirements (for example, internet connectivity, cloud access)
  ○ operating system (for example, open source, proprietary, version).

4.1.5 Factors that affect the energy use, resource efficiency and sustainability of digital systems and devices:
 	
• energy use may include:
  ○ power saving settings
  ○ device usage (for example, time per day)
• resource efficiency may include:
  ○ storage management
  ○ hardware performance (for example, suitability of hardware for task)
• sustainability may include:
  ○ device lifespan
  ○ recycling
  ○ repairability
  ○ disposal.

4.2 System configuration

4.2.1 The interaction between hardware and software components in enabling system functionality:
 	
• relationship and interaction between hardware and software:
  ○ hardware is the physical components
  ○ software provides instructions telling hardware what to do
  ○ hardware needs software to perform tasks
  ○ software needs hardware to execute its instructions
  ○ both components work together to enable system functionality.

4.2.2 The role of digital tools, automation features and automated AI-enabled systems in generating configuration and supporting system setup, and the need to check such outputs for suitability for the intended system: • the role of digital tools to automatically detect hardware and recommend configurations and settings to reduce manual work (for example, device management to automatically install software) • the role of automation features performs tasks automatically instead of requiring someone to do every step manually (for example, installing updates)

DRAFT

Teaching guidance

- the role of AI-enabled systems to analyse information and make recommendations (for example, detect unusual system settings and recommend changes).
- checking automated and AI-generated outputs may include:
  - checking that the recommended settings are suitable for the system
  - checking that the correct software, updates or configurations have been selected
  - checking that automated changes have not caused problems or unexpected effects
  - checking that the output meets the original requirements and is accurate
  - making changes where the recommendation or automated result is not suitable.

Transferable skills

Transferable skills to be demonstrated through this theme:

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

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

- planning:
  - structured activities such as cleaning datasets, developing code, configuring systems and delivering digital systems by identifying steps, sequencing tasks, estimating resources and managing time
- data interpretation:
  - data, systems and digital scenarios by organising information into types, identifying patterns and anomalies, deconstructing problems, and understanding how components interact
- problem solving:
  - evaluating information, data, systems behaviour and AI-enabled outputs by questioning accuracy, weighing the pros and cons, applying logical reasoning and reaching justified conclusions
- evidence-based decision-making:
  - when selecting tools, configurations and solutions, assessing likely impact and justifying recommended actions or improvements
- recording:
  - information accurately by capturing, storing and organising digital content such as datasets, code, configurations, findings and documentation.

Work-related behaviours

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

- organised
- flexible
- committed.

DRAFT

Theme 5: Digital research and evidence-based recommendations

Theme summary		
This theme introduces learners to essential research and evaluation practices. By identifying and assessing the reliability, accuracy and authority of digital sources, learners will develop the foundational skills needed to identify and select digital sources that are relevant to make evidence-based recommendations.		
Assessment		
Assessment by examination (AbE) and non-exam assessment (NEA).		
Mandatory Teaching content must be covered by the tutor during the delivery of this qualification.	**Level 2**	**60 GLH**

Subject topic	Teaching content The learner must know and understand:
5.1 Information reliability	5.1.1 Variation in the reliability, accuracy, authority and purpose of digital information
	5.1.2 The influence of bias within digital information on interpretation and recommendations
	5.1.3 The potential for automated and AI-enabled content generation systems to produce inaccurate, misleading or fabricated information (sometimes referred to as hallucinated outputs), and the need to verify such information against reliable sources
5.2 Evidence-based recommendations	5.2.1 The role of comparing information across multiple sources in supporting accurate conclusions
5.3 Referencing and recording sources	5.3.1 The importance of intellectual property rights, ownership, attribution and appropriate use of digital and AI-generated content
	5.3.2 The role of referencing practices in ensuring transparency and traceability of sources
	5.3.3 The role of workplace procedures governing acknowledgement and recording of information sources

Subject topic	Teaching content The learner must be able to:
5.4 Information reliability	5.4.1 Identify digital sources that are relevant to a defined purpose
	5.4.2 Check information across sources to confirm key points
5.5 Evidence-based recommendations	5.5.1 Select information that directly supports an evidence-based recommendation
	5.5.2 Communicate recommendations clearly, showing how evidence supports conclusions
5.6 Referencing and recording sources	5.6.1 Use search, formatting and checking functions within digital applications to support drafting, reviewing and organising information
	5.6.2 Acknowledge and reference sources used

DRAFT

Teaching guidance
This teaching guidance supports delivery of the mandatory teaching content. While it provides examples, these are not exhaustive.
5.1 Information reliability
5.1.1 Variation in the reliability, accuracy, authority and purpose of digital information: • reliability is how trustworthy and dependable the information is (for example, information from a reputable source is perceived as more reliable than information from an unverified source) • accuracy is how correct and up to date the information is (for example, digital information may contain mistakes, misleading facts or outdated details, so it is important to check whether the information is supported by evidence) • authority is how qualified or knowledgeable the author is on the subject (for example, information written by experts or professionals is usually more authoritative than information written by someone without relevant knowledge) • purpose is the reason why the information has been created or published (for example, digital information may be available to educate, inform, entertain, persuade or advertise).

5.1.2 The influence of bias within digital information on interpretation and recommendations:
 	
• bias occurs when digital information presents a one-sided opinion rather than being fair and balanced, such as:
  ○ personal opinions
  ○ selective information
  ○ advertising/sponsorship
  ○ political
  ○ social influence
  ○ social media algorithms.

5.1.3 The potential for automated and AI-enabled content generation systems to produce inaccurate, misleading or fabricated information (sometimes referred to as hallucinated outputs), and the need to verify such information against reliable sources:
 	
• why this happens (for example, generating a response based on patterns rather than fact)
• why this is a problem (for example, incorrect AI-generated medical advice)
• ways to help identify AI-enabled content (for example, checking whether the information provides reliable sources or evidence)
• why verification is important may include:
  ○ avoiding mistakes
  ○ making informed decisions
  ○ preventing misinformation
  ○ avoiding harmful consequences.

5.2 Evidence-based recommendations

5.2.1 The role of comparing information across multiple sources in supporting accurate conclusions:
 	
• to compare information across multiple sources to help make an accurate and reliable conclusion may include:
  ○ checking accuracy
  ○ identifying mistakes
  ○ identifying bias
  ○ providing different perspectives
  ○ confirming findings
  ○ identifying outdated information.

5.3 Referencing and recording sources

DRAFT

Teaching guidance

5.3.1 The importance of intellectual property rights, ownership, attribution and appropriate use of digital and AI-generated content:

- intellectual property rights protect people's original creations, helping to prevent others from copying/using someone's work without permission
- ownership identifies who has rights over digital content and how their work is shared, copied or used
- attribution means giving credit to the original creator when using their work, such as naming the author or providing a link to the original source
- appropriate use of digital content means that:
  - digital content should be used responsibly
  - users should:
    - check permissions
    - follow copyright rules
    - avoid plagiarism
- AI-generated content should be used responsibly and transparently.

Transferable skills

Transferable skills to be demonstrated through this theme:

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

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

- problem solving:
  - evaluating information, data, systems behaviour and AI-enabled outputs by questioning accuracy, weighing the pros and cons, applying logical reasoning and reaching justified conclusions
- communicating:
  - findings, risks and recommendations clearly using written, visual and digital formats, adapting explanations and terminology to suit purpose and audience
- investigating:
  - suitable digital sources, interrogating datasets, reviewing logs and dashboards, and designing and carrying out tests to confirm accuracy, function or security
- evidence-based decision-making:
  - when selecting tools, configurations and solutions, assessing likely impact and justifying recommended actions or improvements
- evaluating:
  - processes, evidence and outcomes by reviewing effectiveness, appraising accuracy and reliability, and making recommendations for improvement.

Work-related behaviours

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

DRAFT

Work-related behaviours
• perceptive • reflective.

DRAFT

Section 3: key terms and definitions

Glossary of terms

This glossary provides the Department for Education (DfE) definitions of subject terms relevant to this qualification. Not all terms appear in the teaching content.

Access control	The methods and rules used to determine which users, devices or systems are permitted to access data, systems or services, and the level of access they are allowed.
Access permission	A setting that controls which users, devices or systems are allowed to view, use or modify specific data, systems or services.
Algorithm	A defined sequence of instructions that a computer follows to process inputs and produce an output or solve a problem.
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.
Authentication	A security process used to confirm the identity of a user, device or system before access to data, systems or services is granted.
Automated and AI-enabled systems	Digital tools or systems that use automated processes, artificial intelligence or both to generate, support or refine outputs.
Automation	The use of programmed instructions or scripts that allow digital systems to perform tasks or processes automatically with limited human intervention.
Availability	The condition in which information, systems or services are accessible and usable by authorised users when required.
Brief	A statement that defines a task, including its purpose, requirements, constraints and intended outcome.
Chart	A graphical representation of data used to show patterns, comparisons or relationships between values.
Code	Instructions written in a programming or scripting language that tell a computer how to perform specific tasks or operations.
Component	A hardware or software element that forms part of a larger digital system and contributes to its operation.
Confidentiality	The protection of information so that it is only accessible to authorised users and is not disclosed to unauthorised individuals or systems.
Configuration	The process of setting or adjusting parameters in hardware or software so that a system operates correctly and securely for its intended purpose.

DRAFT

Control (security control)	A measure, safeguard or procedure designed to reduce risks to systems, services or data.
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.
Digital network	A group of connected devices and infrastructure that communicate with each other to exchange data and provide access to digital services.
Digital system	A set of connected components, including hardware, software, data, networks and users, which work together to deliver a digital function or service.
Digital tool	Software, application or digital feature used to support the completion of a task.
Error	A mistake or fault in code, data or configuration that causes a system or program to produce an incorrect or unexpected result.
Functional	Operating correctly and producing the intended result for a designed purpose.
Integrity	The accuracy, completeness and reliability of data, ensuring that information has not been altered in an unauthorised way.
Logical	Based on clear and ordered reasoning in which steps follow a defined and consistent sequence.
Maintenance	Activities such as updates, checks, repairs or adjustments carried out to ensure that systems continue to operate effectively.
Passphrase	A sequence of words used to verify identity and allow secure access to a system, device or service.
Pattern	A repeated or noticeable relationship or trend within data.
Program	A complete set of code that performs a specific function or set of tasks when executed by a computer.
Programming	The process of designing, writing, testing and refining code to create a digital solution that meets a defined purpose.
Protocol	A defined set of rules that governs how data is transmitted and received between devices or systems.
Recommendation	A proposed course of action that is supported by analysis, evidence or evaluation.
Reliability (of a source)	The degree to which information from a source can be trusted as accurate, credible and appropriate for the intended purpose.

DRAFT

Risk	The possibility that an event or action may cause harm, loss or disruption to systems, data or services.
Secure handling	Managing data, devices or systems in ways that prevent unauthorised access, loss, misuse or disclosure.
Sequencing	Arranging tasks, instructions or steps in the correct logical order so that a process operates as intended.
Source (digital source)	A location from which information, data or code is obtained.
Test	An activity carried out to check whether a system, program or component behaves as expected.
Visualise	To present information or data in graphical or pictorial form to support interpretation and understanding.
Vulnerability	A weakness in a system, configuration, process or control that could be exploited to compromise security, functionality or reliability.

Digital technology abbreviations

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

AI	Artificial intelligence
API	Application Programming Interface
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESD	Electrostatic Discharge
GPU	Graphics Processing Unit
HDD	Hard Disk Drive
HTTP/HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
IDE	Integrated Development Environment
MFA	Multi-factor authentication
PIN	Personal Identification Number
RAM	Random-Access Memory
RBAC	Role-Based Access Control

DRAFT

SDLC	Software Development Life Cycle
SSD	Solid State Drive
TCP/IP	Transmission Control Protocol/Internet Protocol
WAP	Wireless Access Point

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.

Products to support the delivery of this qualification may be available. For more information about these resources and how to access them, please visit the NCFE website.

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 November 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.

Mandatory themes

Theme number	Theme title	Level	GLH
1	Preparing and visualising data	2	60
2	System configuration and security	2	60
3	Plan, develop and test a programming solution	2	60
4	Plan and configure hardware and software	2	60
5	Digital research and evidence-based recommendations	2	60

DRAFT

Change history record

Version	Publication date	Description of change

DRAFT