



Department
for Education

Digital Systems and Data

Level 3 V Level subject content

July 2026

Contents

1. Introduction	3
2. Aims	4
2.1 Progression	5
3. Subject Content	6
3.1 Guidance for awarding organisations	6
3.2 Optionality	6
3.3 Work-related purposes	7
3.4 Core Knowledge and Understanding	18
Annex	20
Glossary of Terms	20
Transferable Skills	23
Workplace behaviours	24
Links to Occupational Standards	25
Links to Foundation Certificates	25

1. Introduction

V Level subject content sets out the knowledge, understanding and skills common to all V Level qualification specifications in this subject. The content provides the framework within which awarding organisations create detailed specifications.

This subject content is grounded in the principles which underpin digital systems, data and solution design as the conceptual foundation for applied digital practice. Students develop the ability to interpret, analyse and apply digital concepts in order to configure systems, work with data, identify risks and design digital solutions within defined contexts.

Digital Systems and Data is positioned as the applied use of systems, data and technologies to meet user needs, rather than as preparation for a specific occupational role or specialism. The emphasis is on understanding how digital systems function, how they are used, and how decisions are made when working with them in organisational contexts.

The Department does not set mandatory prior learning requirements for V Levels. As V Level content is set at level 3, providers will set their own entry requirements at level 2, including any GCSEs required.

2. Aims

This content enables students to develop and apply knowledge, understanding and skills in digital systems, data and solution design. It supports students to interpret, analyse and apply digital concepts within defined contexts, and to use that understanding to inform decisions and solve problems. The content provides a broad level 3 foundation that supports progression to further study and apprenticeships.

Organisational scenarios used within the content should be varied and inclusive, drawing on examples from a range of sectors, local labour markets and organisational contexts to avoid reliance on prior workplace experience or sector-specific knowledge.

Teaching and learning materials developed by awarding organisations should, where possible, reflect a diverse range of users, organisations and digital contexts, including consideration of accessibility, inclusivity and responsible digital practice.

The purpose of this qualification is to enable students to:

Apply their knowledge, skills and understanding to achieve the following work-related purposes (WRP):

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

Through this, develop transferable skills¹, including:

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

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

- digital systems and their components
- data and information and their analysis
- cyber security principles
- system configuration and testing

¹ Please refer to the [Framework for Transferable Skills and Work-related Behaviours](#)

- principles of problem solving and solution design
- usability and accessibility
- ethical and responsible use of digital technologies

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

2.1 Progression

V Levels aim to encourage motivation and interest in pursuing careers and further study related to digital systems and practices, by providing a broad and applied understanding of this, without requiring early occupational specialisation.

The content provides both a strong conceptual foundation for the subject and the basis for developing in-depth understanding of digital systems, data and digital solutions through applying knowledge and skills to achieve work-related purposes.

This combination of theory and practice should secure access to a wide range of higher-level study and training across multiple sectors, including those related to computing, information technology, data science and related digital disciplines.

3. Subject Content

3.1 Guidance for awarding organisations

Inclusion of content in qualification specifications

All the content outlined in this document must be included in qualification specifications.

Lists of content which start with a colon ‘:’

This denotes that all the content in the list is compulsory and is expected to be included in awarding organisations’ qualification specifications.

Lists of content which start with ‘including’

This denotes that all the content in the list is compulsory and is expected to be included in awarding organisations’ qualification specifications. The list is a minimum; awarding organisations can choose to add to the list. To ensure comparability between awarding organisations’ qualification specifications in a subject, DfE will use this approach in limited instances where additional relevant content could reasonably be added without affecting the comparability of qualification specifications and assessments.

Use of ‘e.g.’

This is used to exemplify what is meant by the content statement. It is used to ensure awarding organisations have a clear and consistent understanding of the term; to signal that the example in use now may be superseded by more up-to-date examples; or where different examples could reasonably be included without affecting the comparability of qualification specifications and assessments. Awarding organisations can use the cited example, where it remains relevant and appropriate.

3.2 Optionality

Awarding organisations must develop qualification specifications that include all work-related purposes (WRP1, WRP2, WRP3 and WRP4) and the Core Knowledge and Understanding.

Qualification specifications must make clear that all students must complete the core knowledge and understanding, WRP1 and WRP2, and **one** of either WRP3 or WRP4.

WRP3 and WRP4 are equivalent optional work-related purposes and should be comparable in level of demand and guided learning hours. Students should apply the same core digital knowledge, skills and understanding, using approaches that are appropriate to the defined work-related purpose.

3.3 Work-related purposes

Students are expected to apply knowledge, understanding and skills to achieve authentic work-related purposes. Content specified in this section is expected to be demonstrated through applied activity.

When developing qualification specifications, awarding organisations must allocate between 220 and 260 guided learning hours (GLH) to the development of applied knowledge, understanding and skills directly needed to achieve the defined work-related purposes.

WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making

To achieve this work-related purpose, students must apply knowledge and understanding through preparing, analysing, interpreting and presenting data from different sources in order to produce justified insights that inform decision making within defined contexts.

To do this, students are expected to apply the following knowledge and understanding:

- the purpose of preparing, analysing, interpreting and presenting data to generate insights that support conclusions and decision making in workplace contexts
- how data is structured, formatted and defined within datasets from different sources, including how levels of detail affect interpretation, comparability and use
- data quality issues arising from missing data, duplicate records, inconsistent formats and conflicting values across sources and their impact on analysis
- methods used to validate and prepare data prior to analysis through checking formats and data types, confirming completeness, verifying value ranges and resolving inconsistencies
- analytical techniques used to examine prepared datasets: sorting, filtering, and grouping records; calculating totals, averages and 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
- the role of automated and AI-enabled analytical systems in supporting pattern identification and insight generation, and the need to interpret outputs critically
- the forms and uses of analytical outputs, including summaries, comparisons, trends and indicators, and how these inform conclusions and decision making
- how combining datasets from different sources can reveal relationships and insights not visible when sources are analysed separately, including risks associated with inconsistent definitions and alignment across sources
- the role of metadata, field definitions and documentation in supporting analysis, transparency, accountability and correct interpretation of analysed outputs
- 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
- the relationship between data preparation, analytical methods and the reliability of conclusions
- the relationship between data quality, analytical approach, data limitations, uncertainty and confidence in conclusions, including the impact of outliers, sampling bias and unrepresentative data
- the impact of bias, incompleteness and lack of representativeness in data on analytical outcomes and interpretation

- limitations of datasets used in automated and AI-enabled analysis and potential sources of bias in data collection, preparation, processing and when drawing conclusions
- 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, and accuracy, fairness and mitigation of bias in data and analytical processes
- the importance of transparency when presenting insights generated and supported by automated and AI-enabled systems
- how automated visualisation tools may influence interpretation of findings, including the influence of scale, proportion and representation
- the consequences of presenting automated outputs without explaining assumptions, limitations and confidence in the underlying data and analysis
- how workplace setting, audience needs and decision-making purpose influence the selection of presentation formats
- principles of visual communication that support accurate, transparent, proportionate and non-misleading representation of analysed data findings
- the relationship between analytical findings and presentation choices and user interpretation of information
- the role of interpretation and professional judgement in transforming analytical results into meaningful conclusions, including distinguishing correlation from meaningful relationships
- principles of inclusive and unbiased data handling that support fair, accurate and responsible interpretation of analytical findings, including 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
- inclusive and accessible presentation practices that support understanding by diverse users and audiences
- sustainability considerations relating to the preparation, storage and sharing of data outputs

In working to achieve the work-related purpose, students must be able to:

- interpret a defined analytical and decision-making purpose
- examine data from different sources to determine suitability for analysis
- prepare data for analysis through validation, checking formats and confirming completeness
- analyse prepared datasets to identify patterns, relationships and trends
- examine analytical outputs in relation to the defined purpose

- interpret analytical findings and consider potential sources of bias and limitation in the data
- draw reasoned conclusions from analysed data
- select and apply graphical and tabular visualisation formats to present analysed insights clearly and accurately
- ensure presented outputs are accurate, clearly labelled and transparent about data sources, assumptions and limitations
- communicate analytical findings, insights and conclusions clearly to technical and non-technical audiences
- document analytical decisions, assumptions and outputs clearly
- review presented outputs to improve clarity, accessibility and relevance

WRP2: Apply security protocols and interpret system information to detect and escalate cyber security concerns

To achieve this work-related purpose, students must implement security controls and interpret security-related information in order to identify potential cyber threats, apply appropriate protective actions, and escalate concerns in line with defined procedures.

To do this, students are expected to apply the following knowledge and understanding:

- authentication requirements, access controls, update procedures and data protection measures used to protect digital systems and services, including the relationship between authentication strength, usability and security risk, and principles of least privilege
- 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, and reporting and escalation of suspected security incidents
- common cyber security threats: phishing, social engineering, malware, ransomware, unauthorised access attempts, suspicious network behaviour and data loss incidents
- the use of system logs, alert notifications and account activity records to identify indicators of potential cyber security concerns, including correlation of multiple indicators and distinguishing normal system variation from anomalous behaviour
- the relationship between system activity, security-related information and potential cyber security concerns, including uncertainty in interpretation and the need for professional judgement
- the role of baseline system behaviour in identifying deviations and potential threats
- the relationship between security controls, user behaviour and system vulnerabilities
- the implications of different types of cyber threats and the impact of delayed identification and escalation
- 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 and reporting concerns through defined procedures
- 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
- 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
- energy efficiency, data retention management and secure device lifecycle practices relevant to cyber security

In working to achieve the work-related purpose, students must be able to:

- apply authentication requirements, access controls, update procedures and data protection measures to digital systems
- apply configuration actions relating to user accounts, permissions and security settings in line with defined security procedures
- apply procedures for secure access, authentication and system use
- review security-related information to identify slow response times, repeated errors, failed updates and connectivity interruptions, and what these indicate about system quality
- recognise signs of unexpected and anomalous system activity
- use log files, monitoring dashboards and system alerts to view and interpret security-related information
- record observations clearly and accurately
- escalate potential cyber security concerns in line with security procedures
- select and apply protective actions to systems in response to identified risks and system information
- communicate potential security concerns clearly to others
- handle security-related information in line with policies and procedures for privacy and confidentiality

WRP3: Prepare, configure and assure readiness of digital systems to meet user needs (optional)

To achieve this work-related purpose, students must prepare and configure digital systems in response to defined user requirements and 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.

To do this, students are expected to apply the following knowledge and understanding:

- the purpose of testing digital systems and the role of quality assurance in maintaining system performance, security and service reliability
- categories of testing used in workplace contexts that address system functionality, performance, usability, accessibility and security-related behaviours
- 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
- the impact of system performance, reliability and security issues on user experience, productivity and service continuity
- principles of usability and accessibility and their relevance to system performance, reliability and security for diverse users, including the relationship between interface design, interaction patterns and user effectiveness
- the contribution of inclusive and accessible testing practices to reliable digital systems for diverse users
- the role of contemporary digital tools in supporting test planning, identification of patterns in system behaviour and summarisation of findings
- 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
- 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
- the role of workplace policies, standards and compliance requirements in defining testing scope and quality assurance expectations
- the role of system dependencies and component compatibility in ensuring reliable system operation
- the impact of system configuration on performance efficiency and resource utilisation
- the role of controlled, non-live, simulated and training environments in supporting safe and effective configuration practice

- the role of recording and documenting test findings accurately and consistently to support review, accountability and improvement decisions
- the role of digital tools in supporting system preparation, configuration and checking activities
- the role of clear documentation and communication in supporting accurate, consistent and effective system preparation
- the impact of responsible, inclusive and secure configuration practices, and how accessible configuration supports diverse users and reduces barriers to digital participation
- environmental and sustainability considerations associated with system performance and efficient use of digital resources
- the importance of maintaining system integrity through responsible updates, permissions and security settings

In working to achieve the work-related purpose, students must be able to:

- interpret user and system requirements to determine configuration needs and the scope and focus of testing
- prepare and configure digital systems to meet defined needs
- adjust configuration settings relating to user access, connectivity, storage and security to support system functionality and accessibility
- carry out structured tests to confirm system functionality, performance, stability and security-related behaviours
- assess system usability and accessibility against stated user needs
- review system behaviour and outputs to identify deviations from expected outcomes and apply structured fault-finding approaches where required
- record and compare test outcomes against requirements using accurate terminology and structured formats
- evaluate test outcomes in relation to defined requirements to determine whether systems are ready for use or require further adjustment
- identify and correct configuration settings related to user access, connectivity, storage and security that do not meet defined user requirements
- 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
- apply policies relating to configuration and data protection requirements: secure configuration, access permissions, protection of personal information and software updates
- document configuration decisions clearly
- communicate configuration outcomes clearly and respond to queries in line with workplace procedures
- maintain system integrity through responsible configuration practices, updates, permissions and security settings

WRP4: Design and create a digital solution to meet defined user needs (optional)

To achieve this work-related purpose, students must analyse user needs and design and create structured digital solutions that address defined requirements, constraints and governance expectations.

Digital solutions may include configurable, scripted, automated or low-code approaches; students are not required to use a specific technology, platform or programming language.

To do this, students are expected to apply the following knowledge and understanding:

- the purpose of analysing user needs and requirements when designing digital solutions
- approaches used to define problems, determine solution scope and identify constraints, including identifying user needs and requirements, distinguishing between essential and desirable features, identifying assumptions and dependencies, recognising technical, organisational and resource constraints, distinguishing between stated requirements and underlying user needs
- how digital systems, components and processes influence the feasibility and structure of proposed solutions, including trade-offs between functionality, complexity and maintainability
- the role of automated and AI-enabled systems in supporting solution design, including generating, refining and evaluating solution approaches, and the need to assess the suitability and limitations of outputs
- the role of structured logic and step-by-step processes in designing digital solutions to define how inputs, processes and outputs are organised, including the relationship between logic structure and predictability of outcomes
- principles of algorithms, and structured coding approaches used to represent, sequence and control solution logic within digital designs
- the purpose and characteristics of low-code and block-based development approaches, including how they support rapid prototyping, iterative design and early-stage exploration of digital solution ideas
- principles, concepts and approaches underpinning digital design and structured logic in low-code and block-based environments, including abstraction, decomposition, sequencing, selection and iteration, and how these support the development of reliable and maintainable digital solutions
- principles of user experience and user interface design that support usability and accessibility, including the relationship between interface design and user behaviour
- the role of requirements, assumptions and success criteria in shaping solution proposals, including validation of assumptions and their impact on solution effectiveness

- the purpose of low-fidelity representations in communicating solution ideas during early stages of design
- 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
- governance requirements relevant to digital solutions that use automated and AI-enabled systems
- potential risks associated with automated decision-making in digital systems and their implications for users and organisations, including limitations of automated decision-making and the need for human oversight
- the relationship between user needs, workplace context and effective digital solution design
- the contribution of structured problem-solving and logical thinking to robust solution proposals
- how design decisions influence usability, accessibility and system behaviour in digital solutions
- the role of analysis and planning in reducing risk during later stages of development
- 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
- the implications of incorporating automated and AI-enabled processes into digital solutions
- the importance of oversight, accountability and transparency in digital solution design
- the role of documentation and shared understanding in enabling development decisions
- sustainability considerations in digital solution design: efficient use of resources, energy consumption and device lifecycle

In working to achieve the work-related purpose, students must be able to:

- interpret defined user needs and requirements to inform solution design
- analyse a problem to identify inputs, outputs, constraints and success criteria
- structure a proposed digital solution using logical steps and processes
- design solution concepts that consider system behaviour, user interaction and accessibility

- produce a clear and structured solution proposal suitable for development
- use appropriate development tools, environments and structured inputs, e.g. prompts for automated and AI-enabled systems, to create, refine or represent a digital solution in line with defined requirements
- represent solution ideas using specified technical formats (e.g. documents, presentations, spreadsheets, databases)
- justify design decisions in relation to user needs and requirements and governance considerations
- document assumptions, decisions and constraints clearly and accurately
- communicate proposed solutions clearly to technical and non-technical audiences

3.4 Core Knowledge and Understanding

When developing qualification specifications, awarding organisations must allocate between 100 and 140 GLH to Core Knowledge and Understanding to ensure sufficient depth of coverage of key digital concepts, theories and principles at level 3.

The Core Knowledge and Understanding both:

- provides the conceptual foundation that underpins achievement of the work-related purposes
- ensures that students develop a coherent understanding of the subject more broadly

Where concepts appear across both core knowledge and understanding and work-related purposes, the core knowledge and understanding section defines what students must understand conceptually, while the work-related purposes specify how that understanding is applied and demonstrated in context.

Students must know and understand:

- the main components of digital systems; hardware, software, network infrastructure, data storage and user interfaces, and their roles within system structure
- the role of operating systems, user accounts and access controls in enabling secure and effective system use
- configuration requirements relating to user accounts, access permissions, connectivity, storage and security settings, including dependency relationships between configuration settings and system behaviour, and the importance of consistency in configuration practices
- the relationship between workplace requirements, user needs, configuration decisions, and system performance, usability and security
- 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
- the relationship between defined requirements, test outcomes and decisions about system readiness for deployment and continued use, including defined performance thresholds and trade-offs between performance, usability and security
- the nature and causes of technical faults in digital systems, including how faults arise from hardware, software, network and user-related factors, and how system behaviour can be interpreted in relation to expected outcomes to support fault identification and resolution
- structured approaches to diagnosing and resolving faults, including the role of diagnostic tools, system information and logical processes in supporting accurate

- identification, decision making, escalation and restoration of system functionality, and the consequences of inaccurate diagnosis or delayed action
- 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, and consideration of the impact of actions on users, services and organisations
 - the implications of using automated and AI-enabled systems in decision-making, including limitations, bias and the need for human oversight
 - the role of communication in technical support, including how information is gathered, interpreted and conveyed to support accurate identification and resolution of issues and effective service delivery
 - how communication approaches influence clarity, efficiency and user experience, including the need to adapt communication to meet diverse user needs and to distinguish between communication-based support and technical troubleshooting activities
 - 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
 - the role of collaboration in developing digital solutions, including how different roles, perspectives and forms of expertise contribute to decision making and the quality of proposed solutions, and how structured approaches to collaborative working support effective and consistent outcomes
 - how user needs are identified, interpreted and translated into digital solution designs, including the role of feedback, iteration and shared understanding in refining solutions
 - principles of problem solving, programming logic and digital solution design, including abstraction, decomposition, sequencing, selection and iteration, and structured approaches used to develop, test and refine digital solutions
 - the role of prompts and structured inputs in generating outputs from automated and AI-enabled systems, including how prompt design influences the relevance, accuracy and limitations of generated outputs and the broader social and ethical implications of automated and AI-enabled systems and their outputs
 - ethical, legal and sustainability considerations relevant to digital practice, including intellectual property rights, ownership, attribution and the responsible use of automated and AI-enabled systems and their outputs
 - the influence of constraints, including technical, organisational and resource factors, on collaborative decision making and digital solution design, and the importance of inclusive and responsible collaboration in achieving effective outcomes

Annex

Glossary of Terms

Term	Definition
Access control	The methods and rules used to determine which users, devices or systems are permitted to access data, systems or services, and the level of access they are allowed.
Accessible	Designed so that people with a wide range of abilities, needs and characteristics can use a system, product or service effectively.
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.
Brief	A statement that defines a task, including its purpose, requirements, constraints and intended outcome.
Component	A hardware or software element that forms part of a larger digital system or product and contributes to its operation.
Compliance	Conformity with defined workplace policies, procedures, regulatory requirements or standards.
Configuration	The process of setting or adjusting parameters in hardware or software so that a system operates correctly and securely for its intended purpose.
Control (security control)	A measure, safeguard or procedure designed to reduce risks to systems, services or data.

Term	Definition
Controlled environment	A physical or virtual environment used to configure, test or modify systems without affecting live operational systems or users.
Data	Recorded information that can be stored, processed, analysed or transmitted by digital systems.
Data validation	Checks carried out to ensure that data is complete, correctly formatted and within expected ranges before it is used.
Dataset	A structured collection of related data items organised so that they can be stored, processed, analysed or presented.
Dependency	A relationship in which one component, process or service relies on another in order to function correctly.
Device	A piece of hardware that performs a computing function or connects to a digital system.
Digital solution	A proposed or implemented way of addressing a need or solving a problem using digital technologies.
Digital system	A set of connected components, including hardware, software, data and users, which work together to deliver a digital function or service.
Documentation conventions	Agreed formats or structures used to record technical information clearly and consistently.
Escalation	The process of referring an issue, fault or concern to a higher level of responsibility in line with defined procedures.
Field definition	Information that describes the name, data type and purpose of a field or column within a dataset.
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.

Term	Definition
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.
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.

Term	Definition
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.

Transferable Skills

The following transferable skills² have been integrated into the content for work-related purposes:

WRP	Transferable skills
WRP1	Analysing when identifying patterns, relationships and trends within datasets and interpreting findings.
WRP1	Decision making when selecting analytical approaches and drawing justified conclusions.
WRP1	Communicating when presenting insights clearly to technical and non-technical audiences.
WRP2	Investigative skills, demonstrated through interpreting system information and monitoring outputs to identify unusual or anomalous behaviour.
WRP2	Decision making when selecting actions and escalation routes in line with defined security procedures.
WRP2	Communicating when reporting observations and potential concerns clearly.
WRP3	Analysing when interpreting user requirements, system information and system behaviour.
WRP3	Decision making when selecting configuration actions in line with defined requirements.
WRP3	Communicating when explaining configuration outcomes clearly.

² Please refer to the [Framework for Transferable Skills and Work-related Behaviours](#)

WRP	Transferable skills
WRP4	Planning when identifying steps, sequencing activities and considering constraints when designing a digital solution.
WRP4	Analysing when examining user needs, system requirements and constraints to structure solutions.
WRP4	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 behaviours² may be developed through student engagement with work-related purposes:

WRP	Workplace behaviours
WRP3	Perceptive when interpreting user requirements, system behaviour and data outputs to identify relevant issues or patterns.
WRP3	Attention to detail when configuring systems, reviewing system information and preparing or analysing data.
WRP3	Focussed when completing structured tasks such as testing, analysis and solution design within defined requirements.
WRP3	Respectful in interactions with others, particularly when handling technical issues or responding to queries.
WRP4	Inclusive in considering diverse user needs, accessibility requirements and fair representation in data and digital solutions.
WRP3	Responsive when addressing system issues, user needs or emerging risks, including appropriate escalation where required.
WRP4	Creative when developing and proposing digital solutions to meet defined user needs and constraints.
WRP4	Adaptable when responding to changing requirements, system behaviour or feedback during problem solving and solution development.
WRP4	Self-aware in recognising limitations, reflecting on decisions and seeking support or clarification when appropriate.

Links to Occupational Standards

The subject content for this V Level draws upon the following Occupational Standards. These are provided for reference, and awarding organisations are not expected to include any further content from these standards or signal content alignment in any more detail in their qualification specifications.

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

Links to Foundation Certificates

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

V Level reference	Foundation Certificate reference	Knowledge and Understanding	Skills
WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making and Core Knowledge and Understanding	LO1: Data handling, analysis and communication	Principles of data handling, data quality, processing and analysis	Preparing, analysing and presenting data to generate insights and support decision making
WRP1: Prepare, analyse, interpret and present data from different sources to support conclusions and decision making	LO6: Evidence-based analysis and decision making	Use of data and evidence to support conclusions and judgements	Interpreting findings and making justified, evidence-based decisions

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



Department
for Education

© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0, except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third-party copyright information, you will need to obtain permission from the copyright holders concerned.

About this publication:

enquiries www.gov.uk/contact-dfe

download www.gov.uk/government/publications

Follow us on X: [@educationgovuk](https://twitter.com/educationgovuk)

Connect with us on Facebook: facebook.com/educating