Certificate in Digital Support L3

Contents

What is this Qualification?

The NCFE Level 3 Certificate in Digital Support is a regulated qualification designed to provide learners with knowledge and skills relevant to the digital support sector.

Key aims and objectives of this course are:

- Understand organisational policies, standards and legislation applicable to the digital support sector and the potential consequences of non-compliance.
- Manage a range of network devices, configure a range of server types and design a network infrastructure.
- Understand the concepts and fundamentals of data, including the purpose and process of backing up data.
- Use a security information and event management (SIEM) software and understand how to establish whether a vulnerability has been exploited.
- Use a system log (syslog) and install, configure and deploy an operating system and software applications.
- Understand digital project management methodologies and working practices, be able to use a range of digital applications, and act as a digital champion by providing end-user support
- This qualification is at **Level 3**.

Who is this Course for?

Prior Knowledge and Suitability:

- There is **no specific prior knowledge** a learner must have to start this qualification.
- However, learners will need to have **good written and spoken English** to successfully complete the course assessments. Learners may also find it helpful if they have previously achieved a Level 2 Digital Skills or Information Technology qualification.

Why Should Learners Enrol?

- **Skills gained include:**
  - Communication and collaboration: writing, verbal and face-to-face skills, audience-appropriate language, active listening, teamwork and stakeholder handling.
  - Problem solving and decision-making: structured approaches (fishbone, 5 Whys, computational thinking), incident/request management, and continuous improvement cycles.
  - Task and time management: prioritising to SLAs, documenting actions, reporting progress and performance.
  - Career development: researching roles, mapping skills/behaviours, and creating a CPD plan for progression.

Guided Learning Hours & Commitment

- **GLH:** 180 hours (taught sessions)
- **Total Qualification Time (TQT):** 198 hours (includes independent study)
- Learners should expect to commit additional time outside of lessons for:
  - Research
  - Assignments
  - Portfolio building

Unit Breakdown

Unit 01: Working in the digital support sector (20 GLH)

Learners will be able to demonstrate core transferable skills applicable to the digital support sector and understand career progression within the sector.

- **Purpose & context:** Understand how the digital support sector operates and why policies, standards and legislation matter for day-to-day work.
- **Legislation, policy and standards:** Recognise relevant UK and international frameworks (for example UK GDPR/DPA 2018, Computer Misuse Act) and common organisational policies (AUP, backup, access control, incident management).
- **Professional skills:** Apply safe working, communication and teamwork practices; explain how good information management improves customer service and operational efficiency.
- **Career development:** Research a target role, identify skills/knowledge/behaviours, and build a CPD plan (chosen role, current skills, entry requirements, skills gaps, required registrations, SWOT, CV).

Unit 02: Network infrastructure and cloud services (40 GLH)
In this unit the learner will be able to manage a range of network devices, configure a range of server types and design a network infrastructure. Threat Intelligence: You will explore the threat intelligence lifecycle and the importance of using reliable and valid sources of Open Source Intelligence (OSINT) data.

- **Manage network devices:** Explain roles and interactions of switches, routers and firewalls in a network architecture. Configure a small network and troubleshoot standard issues; simulation tools permitted.
- **Servers and shared resources:** Explain and (via practice or simulation) configure server types: Directory, DNS, DHCP, file, print, mail, application, database, web/proxy/cache. Describe shared resources such as SAN, MFD, VoIP, IP cameras.
- **Design a network:** Compare bus, ring, star, mesh topologies. Explain addressing features (MAC, IPv4/IPv6, ports, subnets, number systems, FQDN). Produce an annotated network diagram including devices, addressing and servers/clients.
- **Cloud & virtualisation:** Explain SaaS, PaaS, IaaS purposes; weigh benefits/limitations (location, cost, scalability, resilience, maintenance). Describe virtualisation (type 1/type 2 hypervisors), where to apply it (network/server/desktop/OS/data), and pros/cons.

Unit 03: Data management (35 GLH)
In this unit the learner will understand the concepts and fundamentals of data, including the purpose and process of backing up data.

- **Data fundamentals:** Identify common organisational data uses (sector, sales, marketing, finance, employee, customer, usage). Distinguish database vs data lake vs data warehouse and explain storage options (HDD/SSD, NAS/SAN, elastic cloud, cloud DB services).
- **Organising and governing data:** Apply practical rules: accepted file formats (JSON/CSV/JPEG/PNG/MP4/WAV/XML/TAB), directory structures, permissions, naming conventions and version control. Consider sovereignty, security/privacy, cost, volume and technical requirements.
- **Backups:** Classify data (public/internal/confidential/restricted). Explain benefits of backing up; compare full/incremental/differential; set considerations (copies, locations, media, schedules, retention, encryption). Create and execute a backup plan.
- Information systems: Explain benefits and typical systems (payroll, inventory, CRM, POs, timesheets, helpdesk) and their input-process-output-feedback functions.
- **Hands-on dataset task:** Source a secondary dataset (eg gov.uk or Kaggle) with ≥ 500 rows; cleanse/validate using suitable software (eg Excel or Python); save to an appropriate format (eg CSV/XLS). Visualise insights and present clear, labelled outputs.

Unit 04: Digital security (30 GLH)
In this unit, learners will understand the importance of information security management and the mitigation controls used to protect organisational data.

- **Information security management:** Identify sensitive company (eg trade secrets, profit margins) and personal data (eg bank details, HR data). Build and use a data catalogue to locate, describe and protect data. Explain DPIA principles per ICO guidance and core information security principles.
- **Access control:** Describe protocols to control access (authentication/authorisation/accounting) and explain why disciplined ISM protects the organisation. Create a simple data catalogue as evidence.
- **Threats, risk and remediation:** Work with SIEM concepts, understand when a vulnerability is exploited, use a scoring matrix (0–10) and severity ratings, and step through risk management stages (identification, probability, impact, prioritisation, mitigation). Recommend remediation (patch, replace/decommission, air gap, migrate/upgrade, transfer risk).

Unit 05: Supporting digital services (30 GLH)
In this unit, learners will understand common digital problems and helpdesk requests, and will be able to resolve a helpdesk ticket

- **Service desk practice:** Summarise helpdesk functions and ticket lifecycle from log → acknowledge → classify (incident/request) → diagnose (tools/logs) → prioritise → action or escalate → resolve → close. Explain SLA purpose and

performance/progress reporting. Describe 1st/2nd/3rd line roles. Resolve a helpdesk ticket.

- **Common requests & problem solving:** Handle typical requests: passwords, access permissions, user setup, software upgrades/patching, MDM, software installs/licensing. Use tools such as alerts, dashboards, live traces, logs, recovery tools and follow detection-response-intelligence best practice.
- **Syslog:** Explain syslog server purpose/benefits; identify captured info (host IPs, timestamps, event messages, severity labels). Install and configure a syslog server, ensure firewall allowances, and interpret outputs during/after an event.
- **Operating systems & deployment:** Describe common OS (Windows, macOS, Linux, iOS, Android). Explain installation/configuration/deployment requirements (system requirements, hardware configuration, optimisation, security, boot, partitioning, file systems). Use disk images and compare deployment methods; then install, configure and deploy an OS.

Unit 06: Supporting digital transformation (25 GLH)
In this unit, the learner will understand the fundamentals of digital transformation and be able to create a digital strategy.

- **Digital transformation foundations:** Explain what DT is, the barriers, and how to express a simple digital strategy with success measures. Compare agile vs waterfall, outline DevOps/CI-CD, and act as a "digital champion" using common collaboration and communication tools.
- **Benefits to the organisation:** Link transformation to outcomes such as streamlined workflows, reduced costs, productivity gains, better customer satisfaction and less waste; communicate these clearly to stakeholders.

Assessment Method

- Learners will be assessed through a **portfolio of evidence** (6 workbooks, one for each unit), which includes:
  - Written reports
  - Presentations
  - Discussions
  - Assignments
  - Case studies
- All assessments are:
  - **Internally assessed** by tutors.
  - **Externally quality assured** by NCFE.

Career Pathways

After completing the course, learners can progress to:

- Level 4 qualifications in cyber security or IT.
- Entry-level roles such as:
    - First Line IT Support
    - Digital Support Technician
    - Digital Application Technician
    - Service Desk Analyst