



HM Government

T-LEVELS

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 1

Assignment Brief

V1.0

Paper number: P003047

16 March 2026 – 27 March 2026

603/6901/2

NCFE

T Level Technical Qualification in Digital Support Services
Occupational specialism assessment (OSA) (603/6901/2)

Digital Support

Assignment Brief

Assignment 1

Contents

About this assignment.....	3
Scenario	4
Task 1: prepare for installation.....	5
Task 2: install and configure a small network.....	7
Document information	11

About this assignment

Introduction

This assignment is set by NCFE and administered by your provider during a set 2-week window.

The assignment will be completed under supervised conditions.

You must complete all tasks in this assignment independently. You are required to sign a declaration of authenticity to confirm that the work is your own. This is to ensure authenticity and to prevent potential malpractice and maladministration. If any evidence was found not to be your own work, it could impact your overall grade.

Internet access is only allowed for Task 2. Internet access is available for this task to allow you to install, configure and update operating systems and software applications. You are **not** permitted to use the internet for any other purpose, such as research. A copy of your browsing history must be submitted as part of your evidence for this task.

Your provider will provide the licensed software necessary for the tasks.

You have 19 hours to complete all tasks within this assignment. Each task has the following number of hours:

Task 1

8 hours (this task will be spread over 2 days – 1 day for Task 1 (a) and 1 day for Task 1 (b)).

Task 2

11 hours (this will be provided after completion of Task 1. This task will be spread over 3 days. There may be significant periods of time whilst waiting for installations to take place and therefore Task 2 (a), 2 (b) and 2 (c) may be completed in parallel).

Individual tasks must be completed within the timescales stated within each task, but it is up to you how long you spend on each part of the task, therefore be careful to manage your time appropriately.

Marks available across all Assignment 1 tasks: 76.

Details on the marks available are provided in each task.

You should attempt to complete all of the tasks.

Read the instructions provided carefully.

Take all photographs using the digital camera supplied by your provider. Use of personal mobile phones is **not** permitted.

Performance outcomes (POs)

Marks will be awarded against the skills and knowledge performance outcomes:

PO1: Apply procedures and controls to maintain the digital security of an organisation and its data

PO2: Install, configure and support software applications and operating systems

PO3: Discover, evaluate and apply reliable sources of knowledge

Scenario

You are a digital support specialist hired by MetroCaring Health, a private healthcare organisation.

The company is in the process of setting up a new clinic which will offer both in-person and remote health care services. The clinic will need secure systems for both internal use and their remote health care offering.

The client needs your expertise in planning to support remote working capabilities for healthcare professionals to consult patients virtually using a Voice over Internet Protocol (VoIP) system. This will require access to the Telehealth system (technology that supports remote health care assistance) which enables healthcare-related work to be logged centrally and allows remote working.

The client requires you to support with preparing and installing a secure network of computers and mobile devices for the employees to deliver health-related services in-house.

Past Paper

Task 1: prepare for installation

Time limit

8 hours

Task 1 (a) must be completed prior to starting Task 1 (b).

Task 1 (a) is allocated 3 hours 30 minutes.

Task 1 (b) is allocated 4 hours 30 minutes.

You can use the time how you want, but each task must be completed within the time limit.

[20 marks]

Student instructions

Based on the scenario, you must complete the relevant preparation that will enable you to set up:

- 10 workstations
- 4 laptops
- 4 mobile devices
- 1 printer
- 1 router
- 2 switches
- 1 main server
- 1 VoIP server for virtual consultations.

The network is required to be set up within a 2-week window, to ensure all employees are up and running as quickly as possible.

For **Task 1 (a)** you must create a report to explain the security considerations required for the installation, configuration, and support of end-user services to ensure confidentiality, integrity and availability including:

- suitable recommendations on implementing business control techniques within the workplace (physical and administrative)
- explanations on how the client should operate the new data systems effectively, appropriately, and securely, considering the UK General Data Protection Regulation (UK GDPR) / Data Protection Act (DPA) 2018 and its principles.

[8 marks]

For **Task 1 (b)** you must plan and complete the relevant network planning documentation including:

- health and safety risk assessment for the work to be undertaken (worksheet in Appendix 1).
- network planning, including:
 - timescales to allow tracking of tasks
 - network design, including internet protocol (IP) addressing scheme inventory log (worksheet in Appendix 1)
- security risk assessment for the work to be undertaken (worksheet in Appendix 1), according to ISO 27001 principles.

[12 marks]

You will have access to the following equipment:

- a computer with productivity software pre-installed.

Evidence required for submission to NCFE

The following evidence should be submitted:

- summary of all business control documentation required (word processing document (report))
- summary of how to secure data systems effectively (word processing document (report))
- network planning documentation, including timescales and network design (word processing document (report))
- health and safety risk assessment worksheet (Appendix 1 – Workbook – Installation and configuration log)
- inventory log worksheet (Appendix 1 – Workbook – Installation and configuration log)
- security risk assessment worksheet (Appendix 1 – Workbook – Installation and configuration log).

Past Paper

Task 2: install and configure a small network

Time limit

11 hours

You can use this time how you want but all parts of Task 2 must be completed within the time limit.

[56 marks]

Student instructions

The client has asked you to install a new network, against a set of requirements. These devices can be either virtual, physical or emulator.

Nurses will use the computers centrally within the clinic, while consultant doctors will use a mobile device (laptop, tablet or phone) to work remotely via the approved remote working solution.

The computers need to be set up allowing the employees to:

- connect to an Active Directory Domain
- use email, word documents and log patient information in spreadsheets
- access the internet
- use communication tools such as softphone, Zoom or Teams on Microsoft Office 365
- have access to project management software to allow tracking of ongoing hospital projects.

The client wants to ensure there is suitable software installed to mitigate any vulnerabilities to the system, including suitable back up security controls in place.

The client has also asked you to create installation notes for these software installations, to support their staff responsible for IT. Your final task is to create a useable document that guides these individuals through the set up of your system.

You will have access to the following equipment:

- three computers with full administrator rights (virtual / physical machine and software)
- internet access
- operating systems
- word processing and spreadsheet software
- email software
- project management software
- communication software
- mobile device or emulator
- IP address allocations in line with provider's own network IP addressing schema
- digital camera

Task 2 (a)

The healthcare provider is hoping to update the network in the future to allow more flexibility for hybrid working. They are looking to test how the network will work, so require you to set up a small network along with a mobile device for the employees in the company.

You must install and configure a small-scale network consisting of a server and two workstations.

The user details for the employees are as follows:

	Name	Job role	Department
User 1	A. Smith	Clinic Administrator	Health Support
User 2	J. Harper	Consultant Doctor	Healthcare Team 1
User 3	L. Patel	Nurse	Healthcare Team 2

You also need to provide evidence to show you have completed the following actions:

- implemented a physical / virtual network
- included network security measures to prevent the unauthorised access, misuse, modification or denial of a computer, information system or data (CIA and IAAA)
- installed Windows server and created an active directory, setting up necessary user accounts, groups and permissions
- installed suitable software including:
 - productivity (for example, word processing, spreadsheets)
 - email client
 - communication tools (for example, video conferencing software, softphone service)
 - project management software
 - backup security controls
- arranged software licence management (software install log worksheet within Appendix 1 workbook).

You should refer to the IP addressing schema provided by your provider.

Note: In your evidence document, you will need to provide annotated screenshots for the processes you follow, the implementations you make and any explanations for all the key decisions you make. As you do the various tasks, you need to log all the network security measures that have been taken. You must log any software installations you have planned. You must also describe how software licences will be managed in the installation and configuration log (Appendix 1 – Workbook – Installation and configuration log – security risk assessment and software install log worksheets).

[18 marks]

Evidence required for submission to NCFE

The following evidence should be submitted:

- annotated screenshots (if using virtual machines) or photographs (if using physical machines / devices) showing the setup and successful implementation of the network and server / active directory install
- a copy of your browsing history must be submitted as part of your evidence for this task.

For **Task 2 (b)** you must provide evidence of the following for the client:

- installation and setting up a client operating system (OS)
- installation and configuration of back-up security controls
- joining computer to Active Directory Domain
- installing and configuring application software suitable for the client
- implementing back up security controls
- installing / updating device drivers.

Whilst waiting for the installation to take place, set up and configure a WiFi mobile device for network connectivity by:

- configuring a mobile device to include device lock security measures, mobile locator application, enabling location services and cloud back up
- carry out all necessary mobile device OS and application updates including the installation and configuration of anti-virus software.

Note: you will need to provide annotated screenshots / photographs for the processes you follow and any implementations you make. This will include completing the software installation log (worksheet in Appendix 1) and justifying your decisions. You will also need to show evidence of any drivers which require installing, alongside taking screenshots of a device manager. When updating any software / OS, you must evidence that there are no further updates required on the system. The installation may take some time to complete and therefore you should continue with Task 2 (c).

[22 marks]

Evidence required for submission to NCFE

The following evidence should be submitted:

- screenshots (if using virtual machines) or photographs (if using physical machines / devices) showing the setup and successful implementation of software, device driver status and mobile device
- a copy of your browsing history must be submitted as part of your evidence for this task.

For **Task 2 (c)** you must review the installation and configuration notes and log (started in Task 1) then report the following information to the client, making sure it is up to date and correct:

- record of all operating system / software application installations and utilities, upgrades, uninstalls and any major configuration changes
- identify and explain any vulnerabilities detected in the current system set up / network
- recommend actions to mitigate any vulnerabilities found.

Note: you will have been filling in the installation and configuration log (Appendix 1 - workbook) as you have been completing the task. You will need to review what you have done, ensure that all information contained is correct and identify the vulnerabilities and mitigations required.

Apply your communication skills appropriately, using standard English. Use accurate spelling, punctuation and grammar. Consider your target audience.

[16 marks]

Evidence required for submission to NCFE

The following evidence should be submitted:

- completed installation and configuration log (Appendix 1 – Workbook – Installation and configuration log)
- a copy of your browsing history must be submitted as part of your evidence for this task.

Document information

Copyright in this document belongs to, and is used under licence from, the Department for Education, © 2026.

'T-LEVELS' and 'T Level' are registered trade marks of the Department for Education.

NCFE is authorised by the Department for Education to develop and deliver this T Level Technical Qualification.

'NCFE' is a registered trade mark of NCFE.

Past Paper