



HM Government

T-LEVELS

T Level Technical Qualification in Digital Support Services

Occupational specialism assessment (OSA)

Digital Support

Assignment 2

Assignment Brief

V1.0

Paper number: P003048

22 April – 23 April 2026

603/6901/2

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

Digital Support

Assignment Brief

Assignment 2

Contents

About this assignment	3
Scenario	4
Task 1: deal with job requests	5
Task 2: create user instructions	10
Document information	11

About this assignment

Introduction

This assignment will be delivered on set dates and times specified by NCFE and after the window for Assignment 1.

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 available to allow you to install, configure and update operating system, drivers and software. 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 assignment.

You have 5 hours to complete all tasks within this assignment. Each task has the following number of hours:

Task 1

3 hours (this task will be completed in 1 day).

Task 2

2 hours (this will be provided after completion of Task 1 and be completed in 1 day).

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.

Total marks available across all Assignment 2 tasks: 30.

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)

This assessment requires students to:

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 previously assisted the client with preparing and installing computers, mobile devices, and a secure network to support their healthcare operations.

Since the installation, you have been contracted to work within the digital support team to assist with three IT support requests.

In addition, you have also been asked to communicate methods of safeguarding information and troubleshooting techniques.

Past Paper

Task 1: deal with job requests

Time limit

3 hours

You can use this time how you want but both parts of Task 1 must be completed within the time limit.

[18 marks]

Student instructions

You have been provided with three job requests for you to action (pages 7 to 9). You are to read each of the requests and take the appropriate action. You will be provided with a workstation already set up for each request. You must complete each request and evidence each solution.

For each of the jobs, you will need to prioritise the job requests, and log each of them in the incident log (Appendix 2 – Workbook – DS OS – Assignment 2).

You will also need to evidence completion of these job requests in the form of screenshots to demonstrate your actions and explain all your key decisions.

For **Task 1 (a)** you are required to read the job request tickets (pages 7 to 9) and complete the incident log (Appendix 2) to prioritise each of the jobs, from most important to least important. You will need to justify your reasons for prioritising each job in that order.

[3 marks]

For **Task 1 (b)** you are required to read the job request tickets (pages 7 to 9) and take appropriate action as you see fit. Update the incident log to provide details of what you have done once completed, attaching screenshots / photographs with commentary as necessary.

[5 marks per job request = 15 marks in total]

You will have access to the following equipment:

- 1 x workstation for job 3330 set up with:
 - OS installed – full administrator rights
- 1 x workstation for job 3331 set up with:
 - OS installed – full administrator rights
 - no productivity software installed
- 1 x workstation for job 3332 set up with:
 - OS installed – full administrator rights
 - no productivity software installed
- productivity software (word processor and spreadsheet)
- email client (or a link to download)
- anti-virus software (or a link to download)
- virtual private network (VPN) software
- business email address (login details preconfigured)
- internet access
- digital camera
- job request tickets (pages 7 to 9).

Evidence required for submission to NCFE

The following evidence should be submitted:

- you will need to prioritise each of the jobs in order and log each of the requests in the incident log (Appendix 2 – Workbook – DS OS – Assignment 2)
- fault finding / issue evidence (screenshots or photographs) along with commentaries
- internet browsing history.

Past Paper

Job No: 3330

Details:

Username	Isabelle Mings	Time reported	09:00 am
Department	Telehealth	Date reported	25/02/2026
Tel. no	1066	Priority	
Email	Isabelle.Mings@metrocaringhealth.com	Technician	
Job summary	Remote working	Room	N/A

Fault / request

Isabelle, a telehealth nurse at MetroCaring Health, has requested to become a hybrid worker. Starting next week, she will work from home 3 days a week. As Isabelle handles highly sensitive patient records and healthcare data, she is concerned that losing her device could result in a data breach, jeopardising both patient privacy and regulatory compliance under UK General Data Protection Regulation (UK GDPR). Additionally, she manages confidential projects that, if accessed by competitors, could harm the clinic's reputation.

Isabelle requires a secure solution to protect her data and ensure continued access to her email and work while working remotely. A VPN is to be installed to secure data when working from remote wireless networks. As she is not confident with technology, she has asked the IT team to implement the necessary security measures and provide guidance on maintaining her system.

You have been asked to:

- install and configure anti-virus software (for example, Avast or AVG)
- perform a full-system security scan with the anti-virus software
- install VPN software
- verify that all operating system updates and patches are installed
- configure automatic updates to maintain security compliance.

Job No: 3331

Details:

Username	Mohammed Choudry	Time reported	07:50 am
Department	Clinic	Date reported	20/03/2026
Tel. no	8532	Priority	
Email	Mohammed.Choudry@metrocaringhealth.com	Technician	
Job summary	Legacy system	Room	Administrators' office

Fault / request

Mohammed, a clinic co-ordinator who has recently started with the company, has been assigned an older company computer. The system has been freshly set up with the operating system but lacks the essential productivity software required for his role, which involves creating patient information letters and managing clinic schedules.

Furthermore, Mohammed has mentioned that he finds the standard display settings on the screen difficult to read for long periods, which is causing eye strain. He requires the display to be adjusted for better comfort and clarity.

Mohammed is hesitant to update the system, fearing the loss of vital documents stored on the device, despite IT recommendations to update it for improved functionality and security.

Your tasks:

- check for any errors or updates for peripheral devices and install the latest drivers if required to ensure compatibility
- install a productivity suite to provide essential word-processing and spreadsheet software
- configure the system's accessibility and display settings to reduce eye strain by increasing the size of text and apps to 125% for improved readability
- configure Active Hours for Windows updates to ensure updates do not run between 09:00 to 17:00
- provide a brief explanation outlining the benefits of timely updates for system stability and connectivity.

Job No: 3332

Details:

Username	James Nevison	Time reported	16:00 pm
Department	Consultants	Date reported	26/02/2026
Tel. no	6661	Priority	
Email	James.Nevison@metrocaringhealth.com	Technician	
Job summary	No email client installed	Room	N/A

Fault / request

James, a consultant doctor at MetroCaring Health, works remotely when visiting patients and uses his company laptop. Due to problems with the device, it has recently been restored to default factory settings. The device must be configured to meet the clinic's IT and security standards, ensuring BitLocker is in operation.

James will also need to access his emails when working remotely, so an email client should be installed on the device. Finally, a guide is required that explains why it is important that confidential patient information is encrypted.

Your tasks:

- install and configure an email client
- use BitLocker to encrypt a drive and test it working
- provide James with an update on why encryption is important for his work.

Task 2: create user instructions

Time limit

2 hours

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

[12 marks]

Instructions for students

A remote employee has damaged their company-provided device. Until a replacement is available, they will use their personal device under the company's Bring Your Own Device (BYOD) policy. BYOD allows employees to use personal devices (for example, laptops and smartphones) for work purposes. However, the current BYOD policy lacks sufficient detail to ensure company data is adequately protected.

You are required to create an instructional document that explains:

- the importance of UK General Data Protection Regulation (UK GDPR) and the steps an employee should take to protect company data when using their own device under a BYOD policy
- the steps an employee should follow when reporting a breach
- how to notify IT of any issues.

In addition, you need to create an instruction screen share video that demonstrates:

- how to troubleshoot screen and sound issues on the system
- how to install and configure a software firewall
- how to block access to a website using a firewall.

You are required to:

- apply your communication skills appropriately, using standard English
- use accurate spelling, punctuation and grammar
- consider your target audience.

You will have access to the following equipment:

- a workstation set up on the network
- software firewall (or link to where this can be downloaded from)
- screen capturing recording software / equipment
- internet access.

Evidence required for submission to NCFE

The following evidence should be submitted:

- instructional guidance document on the importance of UK GDPR and the steps taken to protect company data when using own device under a BYOD policy, steps that should be followed when reporting a breach and how to notify IT of any issues
- screen share (video file) for troubleshooting screen and sound issues on the system, installing a software firewall and configuring the firewall to block access to a website
- internet browsing history.

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