



Qualification specification

**NCFE Level 2 Certificate in the Principles of
Cyber Security
QN: 603/5853/1**

Contents

Summary of changes	3
Section 1	4
About this qualification	5
Support Handbook	5
Qualification summary	6
Entry guidance	8
Achieving this qualification	8
Units	9
How the qualification is assessed	10
Section 2	11
Unit content and assessment guidance	12
Unit 01 Introduction to cyber security (L/618/1181)	13
Unit 02 Understand terminology used in cyber security (R/618/1182)	16
Unit 03 Understand legal and ethical aspects of cyber security (Y/618/1183)	20
Unit 04 Understand common threats to cyber security (D/618/1184)	23
Unit 05 Understand methods of maintaining cyber security (H/618/1185)	26
Unit 06 Working with others in cyber security (K/618/1186)	28
Assessment guidance	29
Section 3	31
Explanation of terms	32
Section 4	34
Additional information	35
Resource requirements	35
Support for learners	35
Learner's Evidence Tracking Log (LETL)	35
Support for centres	36
Learning resources	36
Contact us	37

Summary of changes

This document summarises the changes to this qualification specification since the last version (Version 1.0 July 2020) Please check the NCFE website for the most recent version.

Version	Publication date	Summary of amendments
v1.0	July 2020	First publication
v1.1	June 2022	<p>Further information added to the how the qualification is assessed section to confirm that unless otherwise stated in this specification, all learners taking this qualification must be assessed in English and all assessment evidence presented for external quality assurance must be in English.</p> <p>Information added to the entry guidance section to advise that registration is at the discretion of the centre, in accordance with equality legislation and should be made on the Portal.</p> <p>Information added to the support handbook section about how to access support handbooks.</p>

Section 1

About this qualification

About this qualification

This Qualification Specification contains details of all the units and assessments required to complete this qualification.

To ensure that you are using the most up-to-date version of this Qualification Specification, please check the version number and date in the page footer against that of the Qualification Specification on the NCFE website.

If you advertise this qualification using a different or shortened name, you must ensure that learners are aware that their final certificate will state the full regulated qualification title.

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.
- 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.

Support Handbook

This qualification specification must be used alongside the mandatory Support Handbook which can be found on the NCFE website, which contains additional supporting information to help with the planning, delivery and assessment.

This qualification specification contains all of the qualification specific information you will need that is not covered in the support handbook.

Qualification summary	
Qualification title	NCFE Level 2 Certificate in the Principles of Cyber Security
Qualification number (QN)	603/5853/1
Aim reference	60358531
Total Qualification Time (TQT)	185
Guided Learning Hours (GLH)	110
Minimum age	16
Qualification purpose	This qualification is designed to provide learners with sector awareness. It will do this by increasing the knowledge and understanding of roles and issues relating to Cyber Security. It will also act as a stepping stone for learners who wish to study cyber security at a higher level.
Aims and objectives	<p>This qualification aims to:</p> <ul style="list-style-type: none"> • focus on the study of the principles of cyber security • offer breadth and depth of study, incorporating a key core of knowledge of cyber security. <p>The objective of this qualification is to:</p> <ul style="list-style-type: none"> • provide learners with knowledge and understanding of the principles of cyber security.
Work/industry placement experience	Work/industry placement experience is not required.
Rules of combination	To be awarded the Level 2 Certificate in the Principles of Cyber Security, learners must successfully complete 6 mandatory units.
Grading	Achieved/Not Yet Achieved.
Assessment method	Internally assessed and externally quality assured portfolio of evidence.

Progression	<p>Learners who achieve this qualification could progress to:</p> <ul style="list-style-type: none">• Level 3 Certificate in Cyber Security Practices• Level 3 Diploma in IT User Skills• Level 3 Award in Cyber Security Leadership• Level 3 Foundation Technical Level IT: Cyber Security.
Regulation information	<p>This is a regulated qualification. The regulated number for this qualification is 603/5853/1.</p>
Funding	<p>This qualification may be eligible for funding. For further guidance on funding, please contact your local funding provider.</p>

Entry guidance

This qualification is designed for those looking to gain a greater understanding of, or build upon their existing knowledge of Cyber Security issues.

Registration is at the discretion of the centre, in accordance with equality legislation, and should be made on the Portal. However, learners should be aged 16 or above to undertake this qualification.

There is no specific prior knowledge a learner must have for this qualification. However, learners may find it helpful if they've already achieved a Level 1 or 2 Digital Skills or Information Technology qualifications.

Centres are responsible for ensuring that this qualification is appropriate for the age and ability of learners. They need to make sure that learners can fulfil the requirements of the learning outcomes and comply with the relevant literacy, numeracy and health and safety aspects of this qualification.

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

Achieving this qualification

To be awarded this qualification, learners are required to successfully achieve 6 mandatory units.

Please refer to the list of units below or the unit summaries in Section 2 for further information.

To achieve this qualification, learners must successfully demonstrate their achievement of all learning outcomes of the units as detailed in this Qualification Specification. A partial certificate may be requested for learners who do not achieve their full qualification but have achieved at least one whole unit.







Units

To make cross-referencing assessment and quality assurance easier, we have used a sequential numbering system in this document for each unit.

The regulated unit number is indicated in brackets for each unit (eg M/100/7116) within Section 2.

 Knowledge only units are indicated by a star. If a unit is not marked with a star, it is a skills unit or contains a mix of knowledge and skills.

Mandatory units

	Unit number	Regulated unit number	Unit title	Level	GLH
	Unit 01	L/618/1181	Introduction to cyber security	2	20
	Unit 02	R/618/1182	Understand terminology used in cyber security	2	15
	Unit 03	Y/618/1183	Understand legal and ethical aspects of cyber security	2	20
	Unit 04	D/618/1184	Understand common threats to cyber security	2	15
	Unit 05	H/618/1185	Understand methods of maintaining cyber security	2	20
	Unit 06	K/618/1186	Working with others in cyber security	2	20

The units above may be available as stand-alone unit programmes. Please visit our website for further information.

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 is internally assessed and externally quality assured.

The assessment consists of one component:

- an internally assessed portfolio of evidence which is assessed by centre staff and externally quality assured by NCFE.

Unless stated otherwise in this qualification specification, all learners taking this qualification must be assessed in English and all assessment evidence presented for external quality assurance must be in English.

Internal assessment

Each learner must create a portfolio of evidence generated from appropriate assessment tasks, which demonstrates achievement of all the learning outcomes associated with each unit. On completion of each unit, learners must declare that the work produced is their own and the Assessor must countersign this. Examples of suitable evidence for the portfolio for each unit are provided in Section 2.

Internally assessed work should be completed by the learner in accordance with the Qualification Specification.

The Tutor must be satisfied that the work produced is the learner's own.

A centre may choose to create their own internal assessment tasks, they should:

- be accessible and lead to objective assessment judgements
- permit and encourage authentic activities where the learner's own work can be clearly judged
- refer to Course File Documents on the NCFE website.

Supervision of learners and your role as an Assessor

Guidance on how to administer the internal assessment and the support you provide to learners can be found on the NCFE website.

Section 2

Unit content and assessment guidance

Unit content and assessment guidance

This section provides details of the structure and content of this qualification.

The types of evidence listed are for guidance purposes only. Within learners' portfolios, other types of evidence are acceptable if all learning outcomes are covered and if the evidence generated can be internally and externally quality assured. For approval of methods of internal assessment other than portfolio building, please contact our Quality Assurance team.

The Explanation of terms explains how the terms used in the unit content are applied to this qualification. This document can be found in Section 3.

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

Unit 01 Introduction to cyber security (L/618/1181)

Unit summary	The learner will gain an understanding of the need for cyber security and the impact of cyber crime. They will also know about the various job functions in the sector and related key skill requirements.
Guided learning hours	20
Level	2
Mandatory/optional	Mandatory

Learning outcome 1**The learner will:**

- 1 Understand motivations for cyber crime

The learner can:

- 1.1 Describe the term 'cyber crime'
- 1.2 Explain the possible motives for cyber crime
- 1.3 Identify potential **threat actors**
- 1.4 Define the terms 'external threat' and 'insider threat'
- 1.5 Explain the possible motivations that could lead to external and insider threats
- 1.6 Explain what is meant by 'targeted' and 'untargeted' attacks

Learning outcome 2**The learner will:**

- 2 Understand the need for cyber security

The learner can:

- 2.1 List common cyber crime vulnerabilities of:
 - an individual
 - **a business**
 - a nation
- 2.2 Describe the potential impact of cyber crime on:
 - an individual
 - **a business**
 - a nation
- 2.3 Explain the importance of cyber security for:
 - an individual
 - **a business**
 - a nation
- 2.4 Explain why cyber security issues should be reported promptly

Learning outcome 3

The learner will:

- 3 Know about job roles within cyber security

The learner can:

- 3.1 Describe the role of **key organisations** in the cyber security industry
- 3.2 Identify general job functions carried out by cyber security professionals
- 3.3 Define the term 'hacking'
- 3.4 Explain the differences between the following types of hacker:
- white-hat
 - black-hat
 - grey-hat
- 3.5 Identify the **key skills** requirements of a cyber security professional
-

Assessment guidance

Delivery and assessment
<p>1.3 Threat actors can include, but are not limited to:</p> <ul style="list-style-type: none"> • individual • company • nation • hacker • hacktivist. <p>1.6 Learners must give a simple explanation of the differences between ‘targeted’ and ‘untargeted’ attacks.</p> <p>2.1–2.3 Business must include:</p> <ul style="list-style-type: none"> • charitable venture • multi organisational (for example NHS) • international. <p>3.1 Key organisations, for example at the time of publication:</p> <ul style="list-style-type: none"> • NCSC (National Centre for Cyber Security) • GCHQ (Government Communications Headquarters) • ICO (Information Commissioners Office). <p>3.2 The learner must identify general job functions carried out by cyber security professionals, these job functions will be present within most roles in computing.</p> <p>3.5 Key skills, as a minimum the learner must cover:</p> <ul style="list-style-type: none"> • communication • analytical skills • IT/digital skills • team working • project management • problem solving. <p>The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.</p>
Types of evidence
<p>Evidence could include:</p> <ul style="list-style-type: none"> • research • learner report • written or oral question and answer • discussion • assignment • presentation.

Unit 02 Understand terminology used in cyber security (R/618/1182)

Unit summary	The learner will understand cyber security terminology, and the concept of social engineering.
Guided learning hours	15
Level	2
Mandatory/optional	Mandatory

Learning outcome 1**The learner will:**

- 1 Understand cyber security terminology

The learner can:

- 1.1 Define what is meant by the following in relation to cyber security:

- hardware
- **software**
- **data management**
- **networking**

- 1.2 Describe the differences between LAN and WAN

- 1.3 Explain the following terms in relation to cyber security:

- vulnerability
- **threat**
- risk
- attack
- protection
- recovery

- 1.4 Describe **organisational strategies** in relation to cyber security

Learning outcome 2**The learner will:**

- 2 Understand current and emerging challenges in cyber security

The learner can:

- 2.1 Give examples of **current and emerging** challenges in cyber security

Learning outcome 3

The learner will:

- 3 Understand what is meant by social engineering

The learner can:

- 3.1 Define the term 'social engineering'
 - 3.2 Explain the benefits of using social engineering to a cyber criminal
 - 3.3 Describe what is meant by 'open source information'
 - 3.4 Identify information a cyber criminal could obtain through open sources
 - 3.5 Describe **techniques** that could be used as part of social engineering
 - 3.6 Identify useful information a cyber criminal could gain through social engineering
-

Assessment guidance

Delivery and assessment

1.1 Learners must define:

- hardware
- **software** – learners must define what is meant by operating systems and applications in terms of cyber security
- **data management** – learners must cover the three components of security: confidentiality, integrity, and accessibility in terms of cyber security. The learner must also include how data protection legislation reinforces these requirements
- **networking** – learners must define LAN (local area network), MAN (Metropolitan area network), and WAN (Wide area network).

1.2 Learners must describe the differences between LAN and WAN, which could include a basic description of networking concepts and network traffic. Packages, such as Cisco Packet Tracer, can be utilised to simulate a networking environment.

1.3 **Threat** must include:

- Denial of Service (DoS) attack
- Distributed Denial of Service (DDoS) attack
- Botnet software
- Trojan
- Ransomware
- Spyware
- Viruses.

Learners must explain all the terms listed in relation to cyber security. They may use a case study or example to help them do this.

1.4 **Organisational strategies** – the learner must include a description of SOC (security operations centre) and NOC (network operations centre).

2.1 **Current and emerging** challenges can include, but are not limited to:

- Internet of Things
- Dark web
- Cloud services
- Deepfakes.

3.1–3.6 The learner must use a ‘real-world’ instance of social engineering to meet the requirements. They could do this by looking at each other’s social media accounts to identify information that could potentially be used to carry out social engineering on their peers. This could also be achieved by carrying out a desk based research task to gather information about a business or individual that could be used to design a social engineering attack.

3.5 **Techniques** should include:

- phishing

- spear phishing
- vishing
- smishing (also known as SMSishing).

The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence

Evidence could include:

- research
- learner report
- presentation
- written or oral question and answer
- discussion
- assignment.

Unit 03 Understand legal and ethical aspects of cyber security (Y/618/1183)

Unit summary	Learners will understand the key legislation related to cyber security and how to maintain data confidentiality and security. They will also understand ethical and unethical conduct within cyber security.
Guided learning hours	20
Level	2
Mandatory/optional	Mandatory

Learning outcome 1**The learner will:**

- 1 Understand key legislation related to cyber security

The learner can:

- 1.1 Summarise key points of **current legislation** related to cyber security to protect:
 - an individual
 - a business
 - a nation

Learning outcome 2**The learner will:**

- 2 Understand procedures to maintain data confidentiality and security

The learner can:

- 2.1 Describe ways to **protect** stored data
- 2.2 Explain **basic techniques** for encrypting information
- 2.3 Describe the advantages and disadvantages of each encryption technique
- 2.4 Define what is meant by the following:
 - data in transit
 - data at rest
- 2.5 Explain the **security checks** an organisation might undertake before releasing information

Learning outcome 3**The learner will:**

- 3 Understand ethical conduct in cyber security

The learner can:

- 3.1 Describe **ethical conduct** within cyber security
- 3.2 Describe **unethical conduct** within cyber security

Assessment guidance

Delivery and assessment

1.1 Current legislation - the learner's summary of key points must cover a minimum of three pieces of legislation. Examples include, but are not limited to the following:

- The Computer Misuse Act 1990
- The Data Protection Act 2018
- Official Secrets Act 1989
- The Privacy and Electronic Communications Regulations 2003.

Note that the above will change or be replaced over time and it is important that current and relevant legislation is covered. Learners must relate the information to an individual, a business and a nation.

2.1 Ways to **protect** stored data can include, but are not limited to:

- regular backups
- password system
- anti-malicious software
- operating system updates
- file level and share level security
- encryption.

2.2 Learners must explain the two **basic techniques** for encrypting information:

- symmetric encryption (also called secret key encryption)
- asymmetric encryption (also called public key encryption).

2.5 **Security checks** may include, but are not limited to:

- due diligence checks.

3.1 **Ethical conduct** could include:

- adherence to company IT policy
- maintaining confidentiality
- adherence to applicable laws
- promoting information security
- refraining from conflicts of interest.

3.2 **Unethical conduct** could include:

- sabotage
- disclosing or misusing confidential information
- maliciously injuring the reputation or prospects of an individual or business.

The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence

Evidence could include:

- research
- learner report
- written or oral question and answer
- discussion
- assignment
- presentation.

Unit 04 Understand common threats to cyber security (D/618/1184)

Unit summary	Learners will develop an understanding of malicious software and the ways in which a system can be infected. They will understand common and emerging threats, as well as physical threats to cyber security.
Guided learning hours	15
Level	2
Mandatory/optional	Mandatory

Learning outcome 1**The learner will:**

- 1 Know about common and emerging threats to cyber security

The learner can:

- 1.1 Describe **common and emerging** threats to cyber security

Learning outcome 2**The learner will:**

- 2 Understand what is meant by malicious software

The learner can:

- 2.1 Explain what is meant by **malicious software**
- 2.2 Identify ways in which malicious software can infect a system
- 2.3 Identify methods for removing malicious software from an infected system

Learning outcome 3**The learner will:**

- 3 Understand physical threats to cyber security

The learner can:

- 3.1 Explain why **perimeter access control** is important
- 3.2 Give examples of when check and challenge on the premises may be needed
- 3.3 Identify the possible threats to a business presented by the use of:
 - personal devices
 - removable devices
 - hardware
 - **networking infrastructure**
- 3.4 Give examples of possible threats presented by remote working
- 3.5 Describe **best practice** which can help to minimise physical threats to cyber security

Assessment guidance

Delivery and assessment
<p>1.1 Common and emerging threats can include, but are not limited to:</p> <ul style="list-style-type: none"> • phishing • spear phishing • vishing • smishing • waterholing • synthetic identities. <p>Note that the above will change over time and it is important that current and relevant threats are covered.</p> <p>2.1 Malicious software can include, but is not limited to:</p> <ul style="list-style-type: none"> • Ransomware • Viruses • Spyware • Trojan • Worms. <p>3.1 Perimeter access control – perimeter security and access control systems protect and monitor the external boundary of a business or facility. These systems control access to restricted areas and include the control of people, vehicles and materials through entrances and exits of a controlled area.</p> <p>3.3 Networking infrastructure must include, but is not limited to:</p> <ul style="list-style-type: none"> • open Wi-Fi • routers. <p>3.4 It is important that learners focus on the threats presented by remote working in relation to cyber security (eg damage, loss or theft of equipment); equipment may not have the same level of protection; others being able to access login information or see confidential information, etc.</p> <p>3.5 Best practice could include, but is not limited to:</p> <ul style="list-style-type: none"> • CCTV • access controls (eg locks on doors, keypads, access cards) • ID badges • human firewall (staff training). <p>Learners could carry out an assessment on their workplace or home.</p> <p>The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.</p>
Types of evidence

Evidence could include:

- research
- learner report
- presentation
- written or oral question and answer
- discussion
- assignment.

Unit 05 Understand methods of maintaining cyber security (H/618/1185)

Unit summary	Learners will understand the preventative methods used to maintain cyber security, including the principles of user access control and use of firewalls.
Guided learning hours	20
Level	2
Mandatory	Mandatory

Learning outcome 1**The learner will:**

- 1 Understand preventative methods used to maintain cyber security

The learner can:

- 1.1 Describe routine methods to maintain cyber security
- 1.2 Explain what is meant by vulnerability testing
- 1.3 Explain what is meant by penetration testing
- 1.4 Explain what is meant by security updates
- 1.5 Explain the term 'patching' in relation to cyber security
- 1.6 Explain why cyber security information and maintenance records should be accurate and up-to-date

Learning outcome 2**The learner will:**

- 2 Understand the principles of user access control

The learner can:

- 2.1 Define what is meant by user access control
- 2.2 Identify methods of restricting user access
- 2.3 Explain how to create a user access control system

Learning outcome 3**The learner will:**

- 3 Understand the use of firewalls

The learner can:

- 3.1 Define the term 'firewall'
- 3.2 Describe the key functions of a firewall
- 3.3 Define what is meant by network traffic
- 3.4 Explain the advantages and disadvantages of using a firewall to protect from threats

Assessment guidance

Delivery and assessment

2.3 A scenario approach is suggested to allow learners to explain how to create a user access control system, they could do this by setting up access control on a network or operating system. For example, a cloud based application could be used to set up shared folders. Learners could set various permissions on the folders, taking into consideration how an individual sharing folders may differ from how a business creates access to folders. The explanation must also cover use of usernames and password allocation, and how administrator level access can block users from installing unauthorised applications/software and making system changes that could compromise security.

The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence

Evidence could include:

- research
- learner report
- written or oral question and answer
- assignment
- presentation.

Unit 06 Working with others in cyber security (K/618/1186)

Unit summary	The learner will understand team working and the use of interpersonal skills and communication when working in a cyber security role.
Guided learning hours	20
Level	2
Mandatory	Mandatory

Learning outcome 1**The learner will:**

- 1 Understand team working for cyber security

The learner can:

- 1.1 Describe what is meant by **team dynamics**
- 1.2 Compare the benefits of working with others to working alone
- 1.3 Describe ways in which team members can work together to make use of individual strengths
- 1.4 Identify ways to resolve conflict within a team
- 1.5 Explain how reviewing work activities can support effective teamwork

Learning outcome 2**The learner will:**

- 2 Understand the use of interpersonal skills for working in cyber security

The learner can:

- 2.1 Identify a range of **interpersonal skills** used when working in cyber security
- 2.2 Give examples of when different interpersonal skills might be used when working in cyber security
- 2.3 Describe how working with **others** within an organisation can support cyber security

Learning outcome 3**The learner will:**

- 3 Understand types of written communications used in cyber security

The learner can:

- 3.1 Explain the purpose of **written communications** used in cyber security
- 3.2 Identify the potential **audience** for the written communications used
- 3.3 Identify the type of information that may be included in a written communication
- 3.4 Give examples of the **elements** that support effective written communication

Assessment guidance

Delivery and assessment

1.1 Learners must describe **team dynamics** which could include, but are not limited to:

- working relationships
- personalities within a team.

The learner must include how these may differ in formal and informal settings.

2.1 **Interpersonal skills** could include, but are not limited to:

- listening
- verbal and non-verbal communication
- questioning
- giving information
- respecting others' opinions and views
- giving and receiving feedback
- clarifying
- putting across own views clearly and appropriately.

2.2 The learner must give examples based on the skills they identified in 2.1.

2.3 **Others:** for example, other teams, sections or departments within an organisation.

3.1 **Written communications** could include, but are not limited to:

- vulnerability report
- penetration testing report
- incident report
- internal policy document (specific to cyber security such as a company email or IT use policy).

The learner must cover a minimum of three of the above written communications.

3.2 **Audience** could include, but is not limited to:

- line manager
- senior management
- team members
- all staff.

3.3 The learner must identify the type of information that would be included in one of the written communications they identified in 3.1.

3.4 **Elements** could include, but are not limited to:

- clear purpose
- clear message
- accuracy
- attention to detail

- correct use of spelling, grammar and punctuation
- tone of voice for the intended audience
- layout (eg use of headings, section numbers, bullet points etc).

The Explanation of terms (Section 3) explains how the terms used in the unit content are applied to this qualification.

Types of evidence

Evidence could include:

- research
- learner report
- written or oral question and answer
- assignment
- presentation.

Section 3

Explanation of terms

Explanation of terms

This table explains how the terms used at Level 2 in the unit content are applied to this qualification (not all verbs are used in this qualification).

Apply	Link existing knowledge to new or different situations.
Assess	Consider information in order to make decisions.
Classify	Organise according to specific criteria.
Compare	Examine the subjects in detail looking at similarities and differences.
Define	State the meaning of a word or phrase.
Demonstrate	Show an understanding of the subject or how to apply skills in a practical situation.
Describe	Write about the subject giving detailed information.
Differentiate	Give the differences between two or more things.
Discuss	Write an account giving more than one view or opinion.
Distinguish	Show or recognise the difference between items/ideas/information.
Estimate	Give an approximate decision or opinion using previous knowledge.
Explain	Provide details about the subject with reasons showing how or why. Some responses could include examples.
Give (positive and negative points....)	Provide information showing the advantages and disadvantages of the subject.
Identify	List or name the main points. (Some description may also be necessary to gain higher marks when using compensatory marking).
Illustrate	Give clear information using written examples, pictures or diagrams.
List	Make a list of key words, sentences or comments that focus on the subject.
Plan	Think about and organise information in a logical way. This could be presented as written information, a diagram, an illustration or other suitable formats.
Perform	Do something (take an action/follow an instruction) which the question or task asks or requires.
Provide	Give relevant information about a subject.
Reflect	Learners should look back on their actions, experiences or learning and think about how this could inform their future practice.
Select	Choose for a specific purpose.
Show	Supply sufficient evidence to demonstrate knowledge and understanding.
State	Give the main points clearly in sentences.

Use	Take or apply an item, resource or piece of information as asked in the question or task.
------------	---

Section 4

Additional information

Additional information

Resource requirements

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

- a digital device for example, a desktop PC, laptop or tablet
- access to a storage medium
- web browser software/applications
- internet connectivity
- cyber security related software/applications*

*This is a knowledge only qualification and there is no requirement for the learner to demonstrate any cyber security skills. However, should centres wish to give learners access to software to illustrate cyber security concepts, there is no requirement to use any specific software/applications. Centres are able to use any free or paid-for software/applications.

Support for learners

Learner's Evidence Tracking Log (LETL)

The LETL covers the mandatory units in this qualification and it can help learners keep track of their work. This document can be downloaded free of charge from the Qualifications page on the NCFE website. You do not have to use the LETL – you can devise your own evidence tracking document instead.

Support for centres

Useful websites

Centres may find the following websites helpful for information, materials and resources to assist with the delivery of this qualification.

- National Cyber Security Centre www.ncsc.gov.uk/
 - Government Communication Headquarters www.gchq.gov.uk/
 - Cisco Packet Tracer (networking tool) www.netacad.com/courses/packet-tracer
-

Learning resources

We offer a wide range of learning resources and materials to support the delivery of our qualifications. Please check the Qualifications page on the NCFE website for more information and to see what is available for this qualification.

For more information about these resources and how to access them, please visit the NCFE website.

Contact us

NCFE
Q6
Quorum Park
Benton Lane
Newcastle upon Tyne
NE12 8BT

Tel: 0191 239 8000*

Fax: 0191 239 8001

Email: customersupport@ncfe.org.uk

Websites: www.ncfe.org.uk

NCFE © Copyright 2022 All rights reserved worldwide.

Version 1.1 June 2022

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. 2896700).

CACHE; Council for Awards in Care, Health and Education; and NNEB 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.***