

QUALIFICATION SPECIFICATION



Apprenticeships

Digital

English & Maths

ESOL

Personal & Social Development

Level 1 Award in Cybersecurity

This qualification specification covers the following qualification:

Qualification number	Qualification title
603/6526/2	Gateway Qualifications Level 1 Award in Cybersecurity

Version and date	Change detail	Section/page reference
2.0 (January 2026)	Specification template updated	n/a

The previous version of this qualification specification is available in Prism. Search for the qualification in the Qualification Library and select the 'Documents' tab.

About this qualification specification

Gateway Qualifications is a nationally regulated Awarding Organisation that supports education and training providers through its strong relationships, adaptability and expert team.

This qualification specification contains everything you need to know about this qualification and should be used by everyone involved in the planning, delivery and assessment of the Gateway Qualifications Level 1 Award in Cybersecurity.

This document should be read in conjunction with the Gateway Qualifications' Centre Handbook and other publications available on the website, which contain more detailed guidance on assessment and quality assurance practice.

In order to offer this qualification, you must be a Gateway Qualifications recognised centre and be approved to offer this qualification.

If your centre is not yet recognised, please contact our Business Development team to discuss becoming a Gateway Qualifications recognised centre:

Telephone: 01206 911211
Email: enquiries@gatewayqualifications.org.uk
Website: [Gateway Qualifications](https://www.gatewayqualifications.org.uk)

Contents

Introduction	6
1. Qualification overview.....	7
1.1 Qualification purpose	7
1.2 Aims and objectives	7
1.3 Key information.....	7
1.4 Entry requirements	8
1.5 Progression opportunities	8
1.6 Equity, diversity and inclusion	8
1.7 Resource requirements	9
1.8 Support materials and resources.....	9
1.9 Achieving this qualification	9
1.10 Indicative content.....	9
2. Assessment.....	11
2.1 Assessment overview	11
2.2 Assessment language	11
2.3 Explanation of assessment terms used in this qualification	11
3. Unit details	12
3.1 Mandatory unit.....	12
Understanding cybersecurity	12
4. Quality assurance	16
4.1 Internal quality assurance.....	16
4.2 Sampling.....	16
4.3 Internal standardisation	17
4.4 External quality assurance	17
4.5 Centre monitoring	17
4.6 Quality assuring centre assessment decisions.....	18
4.7 Malpractice and maladministration	18
4.8 Direct claim status	18
4.9 Recognition of prior learning.....	18
4.10 Reasonable adjustments and special considerations.....	19
4.11 Appeals.....	19
5. Glossary of terms	20

Introduction

This qualification has been approved by the Office of Qualifications and Examinations Regulation (Ofqual) that regulates qualifications, examinations and assessments in England.

This qualification is intended to introduce learners to the core concepts of cybercrime and digital protection. It equips learners with foundational knowledge of cybersecurity practices, including routine protective measures, user access control, and the principles behind vulnerability and penetration testing.

This award is ideal for flexible delivery, whether as a stand-alone, bite-sized qualification or as part of a broader curriculum. It can be effectively integrated with other units or qualifications to create coherent learning pathways that support progression in digital and IT skills. This qualification is suitable for learners aged 16 and over.

1. Qualification overview

1.1 Qualification purpose

The purpose of this qualification is to introduce learners to the essential principles and practices that underpin the field of cybersecurity, providing a foundational understanding of cybercrime, the nature of digital threats, and their impact on individuals and organisations. It also aims to prepare learners for progression to higher-level qualifications within the sector or related areas requiring more specialised knowledge, skills, and understanding, and to equip them for employment in cybersecurity or associated fields.

1.2 Aims and objectives

The aim of this qualification is for learners to understand cybercrime, its risks, and the effects it has on individuals and organisations.

The objectives of the qualification are to provide learners with the opportunity to:

- develop an understanding of the motives behind cybercrime and the factors that influence malicious online behaviour
- build awareness of key protective methods used to enhance cybersecurity and reduce digital risks
- gain knowledge of relevant legislation and the principles of ethical conduct within cybersecurity practice
- understand the purpose and importance of user access controls in maintaining secure digital environments

1.3 Key information

Qualification summary	
Qualification title	Gateway Qualifications Level 1 Award in Cybersecurity
Qualification type	Regulated Qualifications Framework (RQF)
Qualification number	603/6526/2
Learning aim reference number	60365262
Level	Level 1
Guided learning hours (GLH)	48
Total qualification time (TQT)	60
Credit value	6
Sector subject area	6.1 Digital technology (practitioners)
Age appropriateness	16-18, 19+

Grading scale	Pass/Fail
Assessment method	Portfolio of Evidence
Regulation information	This qualification is regulated by Ofqual for use in England.

1.4 Entry requirements

There are no specific prior skills/knowledge learners must have for this qualification.

Centres must ensure that learners have the correct information and advice when selecting qualifications to ensure that the qualification will meet their needs.

Centres must ensure that this qualification suits the age and abilities of their learners by ensuring that learners can meet the relevant literacy, numeracy, digital, and health and safety requirements of the qualification.

Learners enrolled on this qualification should not undertake another qualification at the same level with a similar title or content, as this could impact funding eligibility due to duplicated learning.

Centres are responsible for registering learners via the Gateway Qualifications' online registration portal Quartz. Learner registration guidance is available on our website, [Registering learners](#).

1.5 Progression opportunities

On completion of this qualification, learners will be equipped with essential introductory knowledge of cybersecurity, including core principles, threats, and protective measures.

Successful completion of the Level 1 Award in Cybersecurity could allow learners to progress onto:

- Gateway Qualifications Level 2 Award in Cybersecurity
- Gateway Qualifications Level 2 Award/Certificate/Extended Certificate/Diploma in Digital and IT Skills
- Level 2 qualifications in Digital and IT

A full in-depth careers information, advice and guidance session should be completed for learners before, during and after completion of learning, finding them the most appropriate progression pathways unique to them and based on their ability and aspirations.

1.6 Equity, diversity and inclusion

At Gateway Qualifications we aim to create an environment which celebrates differences and strives for equitable opportunities and outcomes for all. More than a mere commitment, this Equity, Diversity, and Inclusion Policy stands as a framework, informing every aspect of the work we do. It is our aim to support our staff and learners of all abilities, ensuring the development, delivery, and awarding of qualifications in a fair and inclusive manner.

Whilst developing our qualifications, we have given due consideration to eliminating discrimination, harassment and victimisation, advancing equality of opportunity, and fostering good relations between people who share a relevant protected characteristic (as defined in the Equality Act 2010) and those who do not.

For full details please see the [Equity, Diversity and Inclusion Policy](#).

1.7 Resource requirements

There are no prescribed resource requirements for this qualification. However, centres must ensure that learners have access to appropriate and sufficient resources to support the achievement of all learning outcomes.

Centres may find it useful to access resources from [Cisco Networking Academy](#).

1.8 Support materials and resources

In addition to this qualification specification, the following resources are available for centres approved to offer the qualification:

- a fully embedded scheme of work
- three session plans
- a session plan template
- an interactive PowerPoint
- a Careers, Information and Guidance (CIAG) document with teaching/delivery support

All resources are embedded in the wider adult curriculum, including Fusion Skills and the Standard Skills Classification (SSC). They use contextualised examples and delivery activities to support sustainability and the United Nations Sustainable Development Goals (UN SDGs). The resources are fully inclusive and include enrichment activities and differentiated scaffolds to add value to learning.

1.9 Achieving this qualification

The qualification will be awarded to learners who successfully demonstrate their achievement of all learning outcomes of the unit in the qualification.

The knowledge and understanding that will be assessed as part of the qualification are set out within the unit details.

To be awarded this qualification learners must successfully achieve the single mandatory unit.

Mandatory unit

Unit reference	Unit title	Unit level	Credit value	GLH
A/651/9222	Understanding cybersecurity	Level 1	6	48

1.10 Indicative content

The examples included within the indicative content are provided as guidance only. They are not exhaustive and should not be regarded as limiting the range of knowledge, skills or understanding that may be taught, developed or assessed. Centres may incorporate additional relevant material, contexts or approaches as appropriate, provided these remain aligned with the stated learning outcomes and overall requirements of the qualification.

2. Assessment

2.1 Assessment overview

The qualification is assessed through a portfolio of evidence which is internally assessed by centre staff and externally quality assured by Gateway Qualifications. For more information, please see the [Centre Guide to Best Practice in Internal Assessment](#).

Each learner must build a portfolio of evidence generated from appropriate assessment tasks which demonstrates achievement of all the learning outcomes associated with the unit.

Assessment guidance is provided for the unit. Assessors may use alternative assessment methods as long as they are fit for purpose, meet the requirements of the qualification and ensure the integrity of the assessment process.

On completion of the unit, learners must declare that the work produced is their own and the Assessor must counter sign this.

Should a learner not achieve the required standard to pass an assessment, further teaching and learning should take place before attempting the assessment again.

The qualification will be awarded to learners who successfully demonstrate their achievement of all learning outcomes of the unit in the qualification.

2.2 Assessment language

This qualification will be assessed in English. All learners work must be in English. British Sign Language can be used where it is permitted for the purpose of a reasonable adjustment.

2.3 Explanation of assessment terms used in this qualification

Gateway Qualifications has produced guidance to support consistent delivery of units across all centres offering our qualifications.

For clarification on how to interpret and deliver the command words used in our assessments, please refer to the Assessment Command Word Definitions document, available on the Gateway Qualifications website [Internal & External Assessment Practice - Gateway Qualifications](#) under Assessment Design.

3. Unit details

3.1 Mandatory unit

Understanding cybersecurity

Unit reference:	A/651/9222
Unit summary:	Learners will develop an understanding of the impact of cybercrime and importance of cybersecurity. They will learn about the protective methods individuals and organisations should use to minimise the impact of cybercrime. They will develop an understanding of user access controls and how they can prevent unauthorised access, data breaches and fraud.
Unit level:	Level 1
GLH:	48
Credit value:	6
Grading method:	Pass/Fail

LEARNING OUTCOMES	ASSESSMENT CRITERIA
The learner will:	The learner can:
1. Understand the motives for cybercrime.	1.1 Identify different types of cybercrime and possible motives. 1.2 Outline how cybercrime can affect individuals and organisations. 1.3 Describe methods used by cybercriminals to defraud individuals and organisations.
2. Understand the importance of protective methods in cybersecurity.	2.1 Identify routine protective methods individuals and organisations can use to maintain cybersecurity. 2.2 Identify why cybersecurity testing is important for organisations.
3. Understand legislation and ethical conduct in cybersecurity.	3.1 Identify legislation, codes of conduct and ethical considerations in cybersecurity. 3.2 Identify why cybersecurity codes of conduct are used by organisations.
4. Understand the role of user access controls in cybersecurity.	4.1 Describe the importance of user access controls. 4.2 Describe how to create user access controls.

Indicative content:

AC 1.1: Types of cybercrime, for example:

- malware attacks
- phishing
- ransomware
- identity theft
- denial-of-service (DoS) attacks
- cyber espionage
- online fraud
- cyberbullying

AC 1.1: Motives, for example:

- steal and misuse data (personal, corporate, or financial information)
- commit fraud
- hack IT systems
- cause disruption to organisations
- cyberextortion (demanding money to prevent a threatened attack)
- ransomware attacks
- Denial of Service (DoS) attacks
- cryptojacking (using someone else's computing resources to mine cryptocurrency)
- cyberespionage (accessing government or company data)

AC 1.2: How cybercrime can affect individuals and organisations, for example:

- financial loss
- identity theft
- emotional distress for individuals
- significant financial losses for organisations due to data breaches
- operational disruption
- legal penalties
- reputational damage
- loss of customer trust
- disruption of IT infrastructures
- long-term financial and operational consequences

AC 1.3: Methods, for example:

- phishing - deceptive emails, websites, and text messages to steal information
- spear phishing - emails used to carry out targeted attacks
- baiting - online and physical social engineering attacks that entice victims with a reward
- malware - victims are tricked into thinking that malware is installed on their computer and reveal information or pay money to have malware removed
- pretexting - uses false identity to trick victims into giving up information
- vishing - urgent voice mails convince victims they need to act quickly to protect themselves from an online risk

AC 2.1: Routine protective methods that individuals and organisations can use to maintain cybersecurity, for example:

- practising online safety principles
- installing and maintaining anti-virus, anti-malware, firewalls, and other security software
- ensuring browser safety (for example, privacy settings, VPN use, incognito mode)
- carrying out regular software updates and system/data backups
- being aware of suspicious emails, attachments, links, and pop-ups
- understanding the difference between http and https when accessing websites
- using strong passwords and protecting them (for example, password managers)
- using Multi-Factor Authentication (MFA) methods
- restricting user access to certain types of information (access control)

AC 2.2 Why cybersecurity testing is important for organisations, for example:

- understanding that testing helps identify vulnerabilities before they can be exploited
- recognising that testing supports the effectiveness of protective methods and security controls
- ensuring systems, data, and networks remain secure and compliant with organisational or legal requirements
- reducing the risk of data breaches, financial loss, and reputational damage
- supporting continuous improvement of cybersecurity measures

AC 3.1: Legislation, for example:

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

AC 3.2: Codes of conduct, for example:

- adherence to organisational IT policies and procedures
- maintaining confidentiality
- compliance with legislation
- awareness of information security

AC 4.1: Importance of user access controls, for example:

- importance of user access controls in protecting organisational data and IT systems
- role of access controls in preventing data breaches, fraud, and compliance violations
- understanding authorised users and user permissions within an organisation
- how limiting access to data helps maintain cybersecurity
- contribution of access controls to preventing cybercrimes and minimising security risks
- maintaining data confidentiality, privacy, and overall security through controlled access

- reducing the likelihood of cyberattacks by restricting unnecessary or unauthorised access
- supporting compliance with legal, regulatory, and organisational requirements

AC 4.2 Create user access controls, for example:

- the hardware and software involved
- the login process
- the identification of roles (administrator, editor, viewer)
- the assigning of permissions to different roles to determine what actions or resources each role can access;
 - administrator: full control over all features and data
 - editor: can create, modify, and delete data
 - viewer: can only view data

Learners should also cover the role and importance of usernames and passwords, and how users can be blocked from performing certain actions, such as, installing unauthorised software and making system changes at Administrator level.

4. Quality assurance

As the portfolio of evidence is assessed by the centre's assessor, the centre must operate an internal quality assurance process. This ensures that qualification standards are being applied consistently within a centre through training, standardisation, sampling of marking and feedback.

4.1 Internal quality assurance

Centres should refer to the online [Centre Handbook](#) for further guidance on staffing requirements.

A centre's internal quality assurance process is led by the Internal Quality Assurer (IQA), who is responsible for identifying and promoting best practices in teaching, learning, and assessment. They are responsible for:

- monitoring assessment practices to ensure they meet our standards
- sampling assessment decisions and learner work to verify accuracy and consistency
- observing assessors and tutors, providing feedback and support for improvement
- facilitating standardisation meetings to align assessment practices across teams
- supporting assessors with professional development and guidance
- identifying and promoting best practices in teaching, learning, and assessment
- handling appeals and complaints related to assessment outcomes
- maintaining detailed records for audits and external quality assurance visits

The portfolio of evidence is subject to internal quality assurance whereby a centre regularly samples and evaluates its assessment practices and decisions, and acts on the findings to ensure consistency and fairness.

To ensure the integrity of the internal quality assurance process, Internal Quality Assurers (IQAs) must not quality assure work that they have assessed.

Assessors must ensure fair assessment and equality of opportunity for the learner within the assessment process. In order to ensure that the assessor is making judgements that are consistent with the rest of the assessment team, they must meet regularly with other assessors and internal quality assurers to discuss assessment decisions.

4.2 Sampling

Sampling is a key element of the internal quality assurance process whereby the IQA:

- uses a risk-based approach to determine what to sample and when
- checks the quality and consistency of each assessor's decisions
- maintains a common standard of marking within the centre over time
- applies methods like vertical sampling (same unit across assessors), horizontal sampling (multiple units from one learner), and diagonal sampling (across units and learners)
- ensures sampling covers all units over time, not just at the end of the assessment process

4.3 Internal standardisation

Internal standardisation is a collaborative process by which tutors and assessors within a centre consider work that they have assessed and, using pre-determined criteria, reach a common agreement on standards as being typical of work at a particular level or grade by comparing samples and providing peer evaluation.

The process of internal quality assurance provides an opportunity for assessors to receive feedback and support, which can help improve their assessment skills. It fosters a culture of continuous improvement and professional development among teaching and assessment staff.

Standardisation will be facilitated by the Centre's IQA and should include all those involved in assessing learner evidence. Centre standardisation events should be held at regular intervals. Centres will be required to keep records of each internal standardisation event, including the date, attendees and notes on any outcomes and actions. Centres will be required to store these records securely for three years, and Gateway Qualifications may ask to see them as part of the centre's quality assurance and monitoring activities.

4.4 External quality assurance

The external quality assurance process for this qualification takes a risk-based approach where external monitoring visits are carried out to review the internal quality systems of centres against key quality standards.

External quality assurance falls into two categories, the first being the quality assurance of the centre's policies and procedures (Centre monitoring) as detailed below, with the second being external sampling of the assessment decisions at qualification level.

4.5 Centre monitoring

Centre monitoring is undertaken by an External Quality Assurer (EQA) allocated to the centre. The EQA plays a critical role in the Gateway Qualifications approach to centre assessment standards scrutiny as they are responsible for:

- validating the centre's procedures for delivery of qualifications and assessment
- completing reports for each visit with clear action points where needed
- carrying out an annual compliance visit
- risk rating centres on the above

The EQA will carry out an initial risk assessment at the centre recognition stage and then annually on an ongoing basis and will give a high/medium/low-risk.

The EQA will arrange the annual quality monitoring visits. These visits:

- monitor the centre's compliance with the centre recognition terms and conditions by reviewing programme documentation and meeting managers and centre staff
- identify any staff development needs
- ensure that all procedures are being complied with through an audit trail, and make sure that the award of certificates of achievement to learners is secure

The EQA will contact the centre in advance of a visit. However, Gateway Qualifications reserves the right to undertake unannounced visits, including during assessment times.

4.6 Quality assuring centre assessment decisions

The external quality assurance process for this qualification involves a risk-based approach where sampling of assessment decisions and internal quality assurance activity to ensure that qualification standards are maintained.

An External Quality Assurer (EQA) will be allocated to the centre to sample the centre's assessment decisions, who will consider whether the sample provides evidence of the following:

- that the standard set out in the units is evidenced and assessment decisions are applied consistently
- appropriate teaching, stimulus, support, or learning materials and resources
- an appropriate internal quality assurance strategy and sampling plans
- appropriate and consistent feedback provided by the assessor to the learner, and by the IQA to the assessor

A report will be completed by the EQA and made available to the Centres once the sampling activity has been completed.

4.7 Malpractice and maladministration

Malpractice is any deliberate activity, neglect, default or other practice that compromises the integrity of the assessment process and/or the validity of certificates. It covers any deliberate actions, neglect, default or other practice that compromises or could compromise:

- the assessment process
- the integrity of a regulated qualification
- the validity of a result or certificate
- the reputation and credibility of Gateway Qualifications
- the qualification to the public at large

Centre staff should be familiar with the [Malpractice and Maladministration Policy and Procedure](#).

4.8 Direct claim status

Direct claim status (DCS) is a status given to centres on an individual qualification basis and allows centres to claim certification without waiting for an external quality assurance activity to take place.

DCS is permitted for this qualification. Refer to the [Direct Claims Status page for further details](#).

4.9 Recognition of prior learning

Recognition of Prior Learning enables recognition of achievement from a range of activities through the knowledge, understanding or skills that learners already possess and so do not need to develop these through a course of learning.

The use of RPL is not permitted for this qualification.

4.10 Reasonable adjustments and special considerations

The following are reasonable adjustments that require permission from Gateway Qualifications prior to assessment.

- adapting assessment materials
- adaptation of the physical environment for access purposes
- adaptation to equipment
- assessment material in an enlarged format or Braille
- assessment material on coloured paper or in audio format
- use of British Sign Language (BSL)
- changing usual assessment arrangements
- extra time, for example, assignment extensions
- reader
- scribe
- use of assistive software
- use of assistive technology
- use of coloured overlays, low vision aids
- use of a different assessment location

If not specifically listed in this section, reasonable adjustments are centre permitted, for details on this Centres should refer to the [Reasonable Adjustments and Special Considerations Centre Guidance](#)

For learners who require special consideration at the point of assessment, complete a Special Consideration Request Form.

4.11 Appeals

Learners who wish to appeal about their assessment results or a decision affecting their learning should either be supported by their Centre or should have exhausted their Centre's own appeals process before appealing to Gateway Qualifications. In the latter case, learners must provide Gateway Qualifications with evidence that they have first appealed to their Centre.

Centres and learners should refer to the [Appeals policy](#) for further information.

5. Glossary of terms

This section provides a concise compilation of frequently used terms and acronyms within our organisation and the broader educational context.

Term	Definition
Assessment Criteria (AC)	The standard a learner is expected to meet to demonstrate that learning outcomes have been met.
Authentication	The process of verifying the identity of a user, device, or system to ensure they are authorised to access specific resources or data.
Cybercrime	Illegal activities conducted via digital systems or the internet, such as hacking, phishing, or identity theft.
Data Breach	An incident where sensitive, private, or confidential data is accessed, disclosed, or stolen without authorisation.
Encryption	The process of converting data into a coded format to prevent unauthorised access, ensuring its confidentiality and security.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Guided Learning Hours (GLH)	The number of hours associated to a qualification/unit relating to the activity of a learner in being taught or instructed by – or otherwise participating in education or training under the immediate guidance or supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training.
Learning Outcomes (LO)	Describes what a learner is expected to know, understand and be able to do as a result of the process of learning.
Malware	Malicious software designed to disrupt, damage, or gain unauthorised access to a computer system, such as viruses, worms, or ransomware.
Phishing	A deceptive tactic where attackers trick individuals into providing sensitive information, such as passwords or financial details, often via fraudulent emails or websites.
Ransomware	A type of malware that encrypts a victim's data, demanding payment (often in cryptocurrency) to restore access to the affected files.
Recognition of Prior Learning (RPL)	A method of assessment that considers whether a learner can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess and do not need to develop through a course of learning.

Total Qualification Time (TQT)	Is the number of notional hours which represents an estimate of the total amount of time that could be reasonably expected to be required for a Learner to achieve and demonstrate the achievement of the level of attainment necessary for the award of the qualification.
Two-Factor Authentication (2FA)	A security measure requiring two different forms of identification to verify a user's identity, such as a password and a text message code.
Vulnerability	A weakness or flaw in a system, software, or network that can be exploited by attackers to gain unauthorised access or cause harm.

