QUALIFICATION SPECIFICATION

gateway qualifications

Cybersecurity (Level 1 - Level 2)

Access to HE
Apprenticeships
Digital
Employability & Enterprise
English & Maths
ESOL
Personal & Social Development
Professional Development
Vocational

This qualification specification covers the following qualifications:

Qualification Number	Qualification Title
603/6526/2	Gateway Qualifications Level 1 Award in Cybersecurity
603/6534/1	Gateway Qualifications Level 2 Award in Cybersecurity

Version and date	Change detail	Section/Page Reference
1.0 (Sep 2020)	n/a	n/a
1.1 (Feb 2023)	Removed address and changed back cover	Page 22

About this qualification specification

This qualification specification is intended for tutors, internal quality assurers, centre quality managers and other staff within Gateway Qualifications recognised centres and/or prospective centres.

It sets out what is required of the learner in order to achieve the qualifications. It also contains information specific to managing and delivering the qualifications including specific quality assurance requirements.

The guide 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 these qualifications you must be a Gateway Qualifications recognised centre and be approved to offer the qualifications.

If your centre is not yet recognised, please contact our Development Team to discuss becoming a Gateway Qualifications Recognised Centre:

Telephone: 01206 911211
Email: enquiries@gatewayqualifications.org.uk
Website: https://www.gatewayqualifications.org.uk/advice-guidance/delivering-our-qualifications/become-recognised-centre/

Contents

1. Qualification Information

1.1 About the qualifications

The qualifications have been approved by the Office of Qualifications and Examinations Regulation (Ofqual) that regulates qualifications, examinations and assessments in England and Qualifications Wales, the regulator of non-degree qualifications and the qualifications system in Wales.

This single unit qualification is designed for learners to learn about cybercrime. They will understand routine protective methods used to maintain cybersecurity including the principles of vulnerability and penetration testing and user access control. While they can easily be offered as stand-alone bite-sized awards, the new qualifications could also be usefully combined with other units or qualifications into meaningful packages of learning.

The single unit within each qualification is also included within Digital and IT Skills qualifications.

1.2 Purpose

The qualification purpose is to:

- prepare learners to progress to a qualification in the same sector or a related area at a higher level or requiring more specific knowledge, skills and understanding
- prepare learners for employment in the sector or a related sector.

1.3 Funding

For information on potential sources of funding in England please visit the Education and Skills Funding Agency:

https://www.gov.uk/government/organisations/education-and-skills-funding-agency

https://www.gov.uk/government/collections/qualifications-approved-for-public-funding

https://hub.fasst.org.uk/Pages/default.aspx
For information regarding potential sources of funding in Wales please visit Qualification Wales:

https://www.qualificationswales.org/

1.4 Geographical coverage

These qualifications are approved by Ofqual to be offered in England and by Qualification Wales to be delivered in Wales.

If a centre based outside England or Wales would like to offer these qualifications, they should make an enquiry to Gateway Qualifications. The qualifications are not available for delivery in Northern Ireland.

1.5 Progression opportunities

This qualification is designed to enable progression into further learning at the same level (e.g. from an award to a certificate in Digital and IT Skills) or to further learning at a higher level.

1.6 Equality, diversity and inclusion

It is Gateway Qualifications' aim that there shall be equal opportunities within this organisation and in all the services it provides and within its recognised centres and via the services they provide and so meet the organisation's legal responsibilities to prevent discrimination.

In particular it is the organisation's intention that there should be no discrimination on the grounds of a protected characteristic including age, disability, gender assignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, sexual orientation. It is acknowledged that this is not an exhaustive list.

2. Learner Entry Requirements

2.1 Key information

Qualification Titles	Gateway Qualifications Level 1 Award in Cybersecurity Gateway Qualifications Level 2 Award in Cybersecurity
Age	Pre-16, 16-18, 19+
Prior qualifications or units	There are no prior qualification requirements for these qualifications.
Prior skills/knowledge/ understanding	There are no prior skills, knowledge or understanding requirements for these qualifications.
Restrictions	There are no restrictions to entry for these qualifications.
Additional requirements/guidance	There are no additional rules or guidance regarding learner entry requirements.

2.2 Access to qualifications for learners with disabilities or specific needs

1. Gateway Qualifications and recognised centres have a responsibility to ensure that the process of assessment is robust and fair and allows the learner to show what they know and can do without compromising the assessment criteria.

2. Gateway Qualification has a duty to permit a reasonable adjustment where an assessment arrangement would put a disabled person at a substantial disadvantage in comparison to someone who is not disabled. Please refer to Section 4.5 Access Arrangement, Reasonable Adjustments and Special Considerations for further details.

2.3 Recruiting learners with integrity

Centres must recruit learners with integrity. They must ensure that learners have the correct information and advice on their selected qualification and that the qualification will meet their needs.

Centres must assess each potential learner and make justifiable and professional judgements about their potential to successfully complete the assessment and achieve the qualification. Such an assessment must identify, where appropriate, the support that will be made available to the learner to facilitate access to the qualification.

3. Qualification Details

3.1 Achievement methodology

The qualification will be awarded to learners who successfully achieve an approved combination of units through a Portfolio of Evidence that has been successfully verified and monitored through Gateway Qualifications' Quality Assurance process. Achievement is therefore determined by successful completion of unit assessment with no further requirement for additional/summative assessment.

3.2 Qualification size

Qualification Title	Total Qualification Time	Guided Learning	Credit Value
Gateway Qualifications Level 1 Award in Cybersecurity	60	48	6
Gateway Qualifications Level 2 Award in Cybersecurity	60	48	6

Total Qualification Time 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.

Total Qualification Time is comprised of the following two elements:

- the number of hours which an awarding organisation has assigned to a qualification for Guided Learning, and

- an estimate of the number of hours a Learner will reasonably be likely to spend in preparation, study or any other form of participation in education or training, including assessment, which takes place by – but, unlike Guided Learning, not under the Immediate Guidance or Supervision of – a lecturer, supervisor, tutor or other appropriate provider of education or training.

3.3 Qualification structure

The qualification requirements are provided below.

The knowledge, skills and understanding that will be assessed as part of the qualification are set out within unit specifications. Unit contents, including the learning outcomes and associated assessment criteria, are published on the Gateway Qualifications website and are also available to download from the qualification library in the online system Prism.

For information on Recognition of Prior Learning/Exempt and Equivalent units please see section **3.4 Recognition of Prior Learning (RPL)**

Gateway Qualifications Level 1 Award in Cybersecurity

Learners must achieve the single mandatory unit.

Mandatory (M)

Unit Number	Title	Level	Credit Value	GLH
Y/618/3631	Cybersecurity	1	6	48

Gateway Qualifications Level 2 Award in Cybersecurity

Learners must achieve the single mandatory unit.

Mandatory (M)

Unit Number	Title	Level	Credit Value	GLH
L/618/3674	Cybersecurity	2	6	48

3.4 Recognition of prior learning

Recognition of Prior Learning (RPL) provides learners and Centres with an alternative assessment method by which a learner's previous achievements can meet the assessment requirements for a unit/qualification through the knowledge, understanding or skills that they already possess and so, do not need to develop these through a course of learning.

It enables the recognition of achievement from a range of activities using any valid assessment methodology. Provided that the assessment requirements of a given unit or qualification have been met, the use of RPL is acceptable to contribute to a unit, units, or a whole qualification according to the RPL criteria for a given qualification.

Qualification Number	Qualification Title	RPL Permitted
603/6526/2	Gateway Qualifications Level 1 Award in Cybersecurity	No
603/6534/1	Gateway Qualifications Level 2 Award in Cybersecurity	No

The process of Recognition for Prior Learning is not applicable to these qualifications.

3.5 Links to other qualifications

These qualifications form part of the Gateway Qualifications' qualifications in Digital and IT Skills.

4 Assessment

4.1 Assessment overview

The assessments must be entirely the learners' own unaided work.

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

4.2 Assessment format

The method of assessment for the qualifications is through a portfolio of evidence.

4.3 Assessment language

The qualifications are assessed in English only.

4.4 Support materials and resources

In addition to this qualification specification, the following resources are available on the Gateway Qualifications website:

- Centre Handbook

4.5 Access Arrangements, Reasonable Adjustments and Special Considerations

Gateway Qualifications and recognised centres have a responsibility to ensure that the process of assessment is robust and fair and allows the learner to show what they know and can do without compromising the assessment criteria. Gateway Qualifications understands its requirement as an awarding organisation to make reasonable adjustments where a learner, who is disabled within the meaning of the Equality Act 2010, would be at a substantial disadvantage in comparison to someone who is not disabled.

Gateway Qualifications has identified reasonable adjustments permissible as detailed below. A reasonable adjustment is unique to an individual and therefore may not be included in the list of available access arrangements.

Centres do not need to apply to Gateway Qualifications for approval of reasonable adjustments unless adaptation of externally set assessments is required.

Learners can have access to all forms of equipment, software and practical assistance, such as a reader or a scribe that reflect their normal way of working within the centre. However, such adjustments must not affect the reliability or validity of assessment outcomes or give

the candidate an assessment advantage over other candidates undertaking the same or similar assessments.

The following adaptations are examples of what may be considered for the purposes of facilitating access, as long as they do not impact on any competence standards being tested:

- 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;
- British Sign Language (BSL);
- changing or adapting the assessment method;
- changing usual assessment arrangements;
- extra time, e.g. assignment extensions;
- language modified assessment material;
- practical assistant;
- prompter;
- providing assistance during assessment;
- reader;
- scribe;
- transcript;
- use of assistive software;
- using assistive technology;
- use of CCTV, coloured overlays, low vision aids;
- use of a different assessment location;
- use of ICT/responses using electronic devices.

It is important to note that not all the adjustments (as above) will be reasonable, permissible or practical in particular situations. The learner may not need, nor be allowed the same adjustment for all assessments.

Learners should be fully involved in any decisions about adjustments/adaptations. This will ensure that individual needs can be met, whilst still bearing in mind the specified assessment criteria for a particular qualification.

All reasonable adjustments made by the centre must be recorded on the Gateway Qualifications' Reasonable Adjustments Form and should be made available to Gateway Qualifications upon request. Guidance on the process for applying for formal adjustments can be found on the Forms and Guidance page of Gateway Qualifications' website.

All adjustments to assessment/s must be authorised by the centre's named Quality Assurance nominee or a member of staff with delegated authority where a centre is permitted to make reasonable adjustments, i.e. for internally marked assessments.

Centres should keep records of adjustments they have permitted and those they have requested from Gateway Qualifications. These records should normally be kept for 3 years following the assessment to which they apply.

It is recommended that centres nominate members of staff to take responsibility for demonstrating the implementation and recording of adjustments to assessments for monitoring by Gateway Qualifications or the regulatory authorities.

Special Considerations

Requests for special consideration should be submitted as soon as possible. Please refer to the Reasonable Adjustments and Special Consideration Policy.

5 Centre Recognition and Qualification Approval

5.1 Centre Recognition

Both centre recognition and qualification approval must be gained before centres are permitted to deliver these qualifications.

Guidance on the centre recognition and qualification approval processes is available on the website: https://www.gatewayqualifications.org.uk/advice-guidance/help-admin-tasks/centre-recognition/

5.2 Centre requirements

Centres must ensure that they have the appropriate resources in place when delivering performance units from vocational areas.

In the delivery of qualification and units to pre-16 learners centres are required to exercise due diligence in respect of the following:

- the learner's needs and access to information and advice about the units offered and how the course of learning will meet their needs;
- the learner's present capacity to undertake the tasks set by tutors, and tutors understanding of how particular tasks accord with the assessment criteria for the unit;
- tutors should be fully conversant with the qualification and unit specification/s offered to learners, where clarification is required the centre should consult with the assigned External Quality Assurer for further advice and guidance in the delivery of units and refer to the Centre Handbook and Reasonable Adjustment and Special Consideration policy and guidance.
- centres will be required to have appropriate and up to date risk assessments and ensure that appropriate support and supervision is provided; appropriate subject specialist knowledge should be consulted where the possibility of harm to learners is identified; this will be monitored through Gateway Qualifications' quality assurance process.
- the centre contact for the unit/qualification being delivered must ensure that all procedures relating to the delivery of the unit/qualification operate effectively in the centre.

5.3 Qualification-specific staffing requirements

For Level 1 qualifications:

Please refer to the Staffing Requirements - Qualification Specific Roles section within the online centre handbook for tutor/assessor/IQA requirements: https://www.gatewayqualifications.org.uk/advice-guidance/delivering-our-qualifications/centre-handbook/quality-compliance/

Internal Quality Assurers in addition to being Tutor/Assessors will have knowledge and experience of carrying out internal quality assurance/verification and will hold a recognised internal quality assurance/verification or be working towards one, examples as follows;

- D34 qualification
- V1 qualification
- Internal Verify Award
- Internal Verification of Credit Based Learning: Continuing Professional Development for Practitioners Award
- Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice
- Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Processes and Practice
- L4 TAQA

For Level 2 qualifications:

Tutor/Assessors must be fully qualified and experienced in the subject area in which they are delivering, details of which must be provided to Gateway Qualifications as part of the Qualification Approval application.

Internal Quality Assurers in addition to being Tutor/Assessors will have knowledge and experience of carrying out internal quality assurance/verification and will hold a recognised internal quality assurance/verification or be working towards one, examples as follows;

- D34 qualification
- V1 qualification
- Internal Verify Award
- Internal Verification of Credit Based Learning: Continuing Professional Development for Practitioners Award
- Level 4 Award in the Internal Quality Assurance of Assessment Processes and Practice
- Level 4 Certificate in Leading the Internal Quality Assurance of Assessment Processes and Practice
- L4 TAQA

6 Quality Assurance

Centres should refer to the online Centre Handbook for further guidance.

The quality assurance process for these qualifications is through risk-based external quality assurance monitoring through reviews of centres' internal quality assurance systems against key quality standards and sampling of assessment decisions and internal quality assurance activity to ensure that qualification standards are maintained.

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:

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

The EQA carries out an initial risk assessment at the centre recognition stage and then annually on an on-going basis using Gateway Qualifications' risk assessment criteria, and gives a high/medium/low risk rating in each of the following categories:

- centre resourcing and arrangements: this includes consideration of centre staffing, induction and training, policies and compliance with our centre agreement
- internal assessment and delivery: including reference to staff knowledge and skills, understanding of requirements, and appropriateness of delivery arrangements; also, delivery of external assessments including invigilation, conduct of assessments and confidentiality (where appropriate)
- internal quality assurance: covering IQA procedures, whether staff are appropriately trained, and standardisation arrangements in place
- learner experience: that embraces appropriateness of initial assessment and learners being on the correct programme, learner induction and course support.

EQAs arrange quality monitoring visits to all recognised centres. 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 completion to learners is secure.

EQAs contact the centre in advance of a visit, however Gateway Qualifications reserves the right to undertake unannounced visits including during assessment times.

EQAs will request information from the centre in advance of a planned visit to help inform the evidence to be reviewed during the visit. Centres are obliged to comply with any requests for access to premises, people and records for the purposes of the monitoring visit. If a centre fails to provide access, then Gateway Qualifications will take appropriate action.

Once a visit date has been agreed, the centre should ensure that the appropriate members of staff attend the meeting, all requested documentation is provided and access to qualification, learner and staff records is available.

If a centre cancels a pre-arranged monitoring visit at short notice the EQA must be satisfied that there was a legitimate reason for the cancellation. If this cannot be established, Gateway Qualifications reserves the right to withhold certification claims until a monitoring visit is completed.

Following the visit, the EQA completes a monitoring report which will be sent to the centre for reference afterwards.

The frequency of the quality monitoring visits will be determined by the volume of learner registrations and the actions arising from previous monitoring activity.
Centres found in breach of these procedures may be subject to sanctions by Gateway Qualifications. Please refer to the Gateway Qualifications Sanctions Policy.
If a centre cancels a pre-arranged monitoring visit at short notice the EQA must be satisfied that there was a legitimate reason for the cancellation. If this cannot be established, Gateway Qualifications reserves the right to withhold certification claims until a monitoring visit is completed.

Following the visit, the EQA completes a monitoring report which will be sent to the centre for reference afterwards.

The frequency of the quality monitoring visits will be determined by the volume of learner registrations and the actions arising from previous monitoring activity.
Centres found in breach of these procedures may be subject to sanctions by Gateway Qualifications. Please refer to the Gateway Qualifications Sanctions Policy.

6.1 Internal Quality Assurance

As the assessments are tutor marked 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. A centre's internal quality assurance process is led by the Internal Quality Assurer (IQA) who is responsible for ensuring that all tutors are marking assessments in line with the standards set by Gateway Qualifications.

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

Standardisation will be facilitated by the Centre's IQA and should include all those involved in marking assessments. Centre standardisation events should be held at regular intervals and to a schedule which reflects delivery patterns and supports the marking of live assessments. 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 reports securely for three years and Gateway Qualifications may ask to see these records as part of the centre quality assurance and monitoring activities.

6.2 Quality assuring centre marking

Once the internal quality assurance process is complete, an EQA will be allocated to a centre to sample the centre marking.

The sample selected is based on the number of learners and the centre's risk rating, derived from centre monitoring.

Evidence of the inconsistent marking and actions taken informs the centre's risk rating and this information will be taken into account with the sampling of future assessments, for example, leading to an increase in sampling size.

6.3 Malpractice

Malpractice is any deliberate activity, neglect, default or other practice that compromises the integrity of the internal and external 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 contents of Gateway Qualifications Malpractice and Maladministration Policy:
https://www.gatewayqualifications.org.uk/wp-content/uploads/2017/10/Malpractice-and-Maladministration-Policy.pdf

6.4 Additional quality assurance requirements

There are no additional internal/external quality assurance requirements for these qualifications.

7 Learner Registration and Results

7.1 Registration

Centres will register learners via the Gateway Qualifications' online registration portal. Learner registration guidance is available on our website, https://www.gatewayqualifications.org.uk/advice-guidance/help-admin-tasks/registering-learners/.

7.2 Awarding

The qualifications will be awarded as Pass or Fail. Learners must pass the assessment to be awarded a Pass.

7.3 Issuing results

Results for learners who do not reach the minimum standard for a pass will be recorded as fail.

7.4 Appeals

Centres must have internal appeal arrangements which learners can access if they wish to appeal against a decision taken by Centres, which will include a named contact at the Centre. These arrangements have to be transparent and accessible in order that appeals from learners can be received, considered and resolved fairly.
Please refer to the Gateway Qualifications' Appeals policy:
https://www.gatewayqualifications.org.uk/wp-content/uploads/2017/09/Appeals-Policy.pdf

7.5 Enquiries

Enquiries about assessment decisions should be made once the centre has followed its internal enquiries and appeal procedures.

Contact details are available on our website:
https://www.gatewayqualifications.org.uk/contact-us/

8 What to do next

For existing centres please contact your named Development Manager or Development Officer.

Tel: 01206 911211

Email: enquiries@gatewayqualifications.org.uk

9 Gateway Qualifications

Gateway Qualifications, a not for profit registered charity, is an Awarding Organisation based in Colchester.

We work with learning providers and industry experts to design and develop qualifications that benefit the learner and the employer.

We support flexible, responsive and quality assured learning opportunities whether it's in the classroom, at work, in the community or through distance learning.

We are recognised by Ofqual, to design, develop and submit qualifications to the Regulated Qualifications Framework (RQF) and Qualification Wales to offer regulated qualifications in Wales.

10 Appendices – Unit Details

Cybersecurity

Unit Number:	Y/618/3631
Level:	Level 1
Credit Value:	6
GLH:	48
Unit Aim:	Learners will learn about cybercrime and the risks and effects it has on individuals and organisations. They will understand routine protective methods used to maintain cybersecurity including the principles of vulnerability and penetration testing and user access control.
Assessment Guidance:	N/A
Grading Guidance:	N/A

This unit has 3 learning outcomes.

LEARNING OUTCOMES	ASSESSMENT CRITERIA
The learner will:	**The learner can:**
1 Know about cybercrime.	1.1 Identify different forms of cybercrime and possible motives. 1.2 Outline how cybercrime can affect individuals and organisations. 1.3 Describe the tactics cybercriminals use to defraud people.
Common forms of cybercrime and motives: • Phishing: using fake email messages to get personal information • Stealing/misusing personal information (identity theft) • Hacking: accessing, shutting down or misusing websites, networks and IT systems • Advocating terrorism-related acts • Email and internet fraud • Theft of financial or card payment data • Theft and sale of corporate data • Cyberextortion (demanding money to prevent a threatened attack) • Ransomware attacks • Denial-of-Service (DoS) attack	

• Cryptojacking (where hackers mine cryptocurrency using resources they do not own) • Cyberespionage (where hackers access government or company data) **AC 1.3:** • Social engineering: relies on human instinct of trust, carefully worded email, voicemail, or text message from a cybercriminal can convince people to transfer money, provide confidential information, or download a file that installs malware. Tactics to defraud: • Phishing: tactics include deceptive emails, websites, and text messages to steal information. • Spear phishing: email is used to carry out targeted attacks against individuals or businesses. • Baiting: an online and physical social engineering attack that promises the victim a reward. • Malware: victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be 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 arrest or other risk. • Learners could refer to a 'real world', for example, by looking at each other's social media accounts to identify information that could potentially be used to defraud their peers.	
2 Know about protective methods to maintain cybersecurity.	2.1 Identify routine protective methods to maintain cybersecurity 2.2 State the importance of cybersecurity testing. 2.3 Set up user access controls.
AC 2.1 • Protective methods: practicing diligence, installing appropriate anti-virus software, installing other appropriate security software, turning on firewall, protecting personal information, browser safety, client software, frequent and regular updating, care with email attachments, not opening pop ups, avoiding emails from unknown sources, not visiting suspect sites, anti-malware software, use and protection of passwords, data protection (personal/financial information), restricting access, regular backups. **AC 2.2:** • Cyber security testing: measures the effectiveness of security measures against a potential attack, can be manual or automated, vulnerability testing to reduce the possibility for intruders (hackers) to get unauthorised access, penetration testing (ethical hacking). • Purpose: to test an IT system, network or web application to find security vulnerabilities that a cybercriminal could exploit. **AC 2.3:** • User access controls: learners could do this by setting up user 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, including some with restricted access.	
3 Know about legislation and codes of conduct related to cybersecurity.	3.1 Identify protections for and responsibilities of individuals and organisations as set out in key legislation.

	3.2 Describe ethical and unethical conduct in relation to cybersecurity.

AC 3.1:

- Current UK legislation that applies to different IT systems and data.
- The principles and requirements of the data protection legislation (The Data Protection Act, 2018, GDPR) and its impact on organisations, IT systems and data.
- Computer Misuse Act 1990, its definitions of illegal practices and the impact it has on organisations, IT systems and data.
- Other legislation could include: Official Secrets Act 1989, The Privacy and Electronic Communications Regulations 2003.

AC 3.2:

- Ethical conduct could include: adherence to organisational IT policies and procedures, maintaining confidentiality, adherence to applicable laws, promoting information security, refraining from conflicts of interest.
- Unethical conduct could include: sabotage, disclosing or misusing confidential information, maliciously injuring the reputation or prospects of an individual or organisation.

Cybersecurity

Unit Number:	L/618/3674
Level:	Level 2
Credit Value:	6
GLH:	48
Unit Aim:	Learners will investigate the accidental and malicious security threats that exist to IT systems and data. They will learn about system vulnerabilities and the tools and techniques used to protect users from risks and potential damage, including loss of data, loss of data integrity and unauthorised access to data.
Assessment Guidance:	N/A
Grading Guidance:	N/A

This unit has 4 learning outcomes.

LEARNING OUTCOMES	ASSESSMENT CRITERIA
The learner will:	**The learner can:**
1 Understand security protection and risk management issues.	1.1 Describe the types of threat to IT systems and data. 1.2 Explain the factors that affect the vulnerability of IT systems and data.
AC 1.1: Internal threats to systems and data may arise from the actions of employees or by an authorised user. Accidental threats: • Accidental damage to physical equipment caused by employee/user • Accidental loss of data/power, unintentional disclosure of data, authorised user action • Physical damage, destruction by fire, flood or other disaster • Risk of bring your own device (BYOD) • Unsafe practices • The use of external storage devices/media • Visiting untrusted websites • Downloading/uploading files to/from the internet • File-sharing applications. Malicious threats: • Malicious damage caused by employee/unauthorised user action	

- Intentional deletion/editing of data and intentional disclosure of data
- Dumpster diving and shoulder surfing
- Theft of equipment or data
- Malicious damage to equipment or data
- Unauthorised access by employees to secure areas in a building
- Unauthorised access to administration functions, security levels and protocols, users overriding security controls
- Risk of BYOD.

External threats to systems and data may arise when the internet is used to access IT systems and data, or as a result of the actions of unauthorised people, malicious software, theft or physical damage.
Malicious software (malware) used to obtain secure information, viruses, worms, Trojans, ransomware, spyware, adware, rootkits, backdoors, botnets, zero-day attacks.
Unauthorised access by individuals, commercial organisations or governments.
Social engineering used to obtain secure information by deception, to include collection of passwords, data theft, scams, phishing, pharming, dumpster diving and shoulder surfing.
Damage or destruction by fire.
Malicious damage to equipment or data.
Evolving threats:

- New threats that are constantly being developed/existing threats that evolve over time.
- Importance of organisations/users applying regular updates either automatically or manually.
- Support and information is available for organisations/users on known hardware and software vulnerabilities from manufacturers' help facilities, user forums, FAQs, online tutorials.

AC 1.2:
Vulnerabilities:

- Types of system: individual devices, including PCs, laptops, mobile devices, portable storage devices, networks, including local area network
- (LAN), wireless local area network (WLAN), file servers, cloud computing systems, online storage, remote server, online software.
- Connection between systems: connection to the internet, connection to internal networks.
- Connection methods: wired/wireless (Wi-Fi, Bluetooth, cellular)
- Interactions between devices: use of storage devices.
- Operating systems: unsupported versions, updates not installed, mobile devices' reliance on original equipment manufacturers (OEM) to update system software, legacy systems.
- Software: zero-day vulnerability, downloads, untrusted sources, illegal copies.
- Users: limitations of understanding.

2 Understand measures to protect IT systems and data from current and evolving threats.	2.1 Explain measures to protect IT systems and data from current and evolving threats. 2.2 Compare different physical security measures used to protect IT systems and data.

AC 2.1:
Software and hardware based protection methods including:

- Antivirus software and detection techniques, virus signatures, heuristic techniques, techniques for dealing with identified threats.

- Software and hardware firewalls and the filtering techniques they use, inbound and outbound rules and network addressing.
- User authentication methods and processes and their advantages and disadvantages: types of biometric authentication (fingerprint, retina, facial recognition), two-step/multi-factor verification (MFA), security tokens, including USB-based keys, knowledge-based authentication, including question and response pairs, certificate-based authentication, digital signature, Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA).
- Login procedures: user name and password, rules for password security, best practice for password complexity/strength, graphical password, password history and time between password changes, account lockout and password reset procedures.
- Access controls to restrict user access to: applications, folders/shared areas, files – files' access rights (read only, full access (read/write/execute), read/write, no access), physical resources (access to peripheral devices).
- Protection of data during transmission: virtual private network (VPN), encryption, digital signatures.
- Encryption of files, folders, disks.
- Precautions that can be taken to secure a wireless local area network (WLAN), including: wireless encryption – wired equivalent privacy (WEP), Wi-Fi protected access (WPA2) and Wi-Fi protected setup (WPS), wireless MAC address filtering and hiding the service set identifier (SSID).

AC 2.2:

- Comparing the types, characteristics, benefits and risks, their advantages and disadvantages, and the effectiveness of different physical security measures used to protect IT systems and data.
- Building and IT/network room security: site security locks, card entry, passcode, biometrics– fingerprint, retina, facial recognition, closed circuit television (CCTV), security staff, alarms.
- Data storage: data protection methods, central storage.
- Backup procedures: selection of data, timing, frequency, media, planned, automated and manual, type (full, differential and incremental), on- site, off-site and cloud data storage.
- User/individual actions: logging out of applications, logging off machines, screen locking, shoulder surfing prevention, shredding documents.

3 Be able to implement measures to protect IT systems and data.	3.1 Create a user access control system to restrict unauthorised access. 3.2 Demonstrate how ethical hacking can be used to protect IT systems and data.

AC 3.1:

- Learners need to create a user access control system 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 also showing how an individual sharing folders may differ to how a business shares folders. Learners should also demonstrate username and password allocation, and how administrator level access can block users from installing unauthorised applications/software and making system changes that could compromise security.

AC 3.2:

• Learners need to show how the use of ethical hacking and penetration tools supports cybersecurity by performing a range of activities such as port scanning, vulnerability scanning and password cracking.	
4 Understand current legal and ethical requirements, and IT security policies and procedures.	4.1 Summarise the legal requirements and IT security policies and procedures that exist to protect IT systems and data. 4.2 Explain ethical and unethical conduct when using IT systems.
AC 4.1: • Current UK legislation that applies to different IT systems and data. • The principles and requirements of the data protection legislation (The Data Protection Act, 2018, GDPR) and its impact on organisations, IT systems and data. • Computer Misuse Act 1990, its definitions of illegal practices and the impact it has on organisations, IT systems and data. • Other legislation could include: Official Secrets Act 1989, The Privacy and Electronic Communications Regulations 2003. • Learners need to be aware IT policies will vary from organisation to organisation but will include procedures that cover the following: • Organisation policies (Acceptable Use Policy): internet and email use, security and password procedures (system making you change password frequently) staff responsibilities for the use of IT systems, staff IT security training. • Backup procedure and policies (advantages and disadvantages and purposes): frequency, media, planned, automated and manual, type (full, differential and incremental), on-site/off-site/cloud. • Data protection and disaster recovery policy. **AC 4.2:** • Ethical conduct could include: adherence to organisational IT policies and procedures, maintaining confidentiality, adherence to applicable laws, promoting information security, refraining from conflicts of interest. • Unethical conduct could include: sabotage, disclosing or misusing confidential information, maliciously injuring the reputation or prospects of an individual or organisation.	

gateway qualifications

enquiries@gatewayqualifications.org.uk
www.gatewayqualifications.org.uk
Tel: 01206 911 211

Charity Registration No. 114282
Registered in England Company No. 5502449