Unit Title: Applying Cyber Security Skills in Learning and Work	
Level:	Two
Credit Value:	3
GLH:	30
OCNLR Unit Code:	CN1/2/LQ/001
Ofqual Unit Reference Number:	F/651/9008

This unit has 3 learning outcomes

LEARNING OUTCOMES	ASSESSMENT CRITERIA
The learner will:	The learner can:
1. Understand how cyber threats affect individuals and organisations.	1.1. Describe different types of cyber threats and how they affect personal, learning, or work situations. 1.2. Explain how cyber security supports safe online behaviour. 1.3. Explain risks or limitations arising from poor cyber-security practices.
2. Know how to choose appropriate cyber safe actions for different situations.	2.1. Compare at least two types of cyber threats and their potential impact. 2.2. Explain the factors to consider when choosing a cyber safe response to a threat. 2.3. Outline ways to check whether a response or action has been effective.
3. Be able to apply cyber safe practices to complete a task.	3.1. Demonstrate how to apply cyber-safe practices while completing a digital task. 3.2. Apply responsible behaviours while completing the task. 3.3. Review the action taken and identify strengths and areas for improvement.

Assessment

The grid below provides suggestions for the types of assessment activities that can be used with the unit attached to provide evidence for the learner's portfolio. Please refer to the OCN London Assessment Guidance document for definitions of each activity and the expectations for assessment practice and evidence for moderation.

Case Study	✓	Project	✓
Written question & answer/test/exam		Role play/simulation	
Essay		Practical demonstration	✓
Report	✓	Group discussion	
Oral question and answer	✓	Performance/exhibition	
Written description	✓	Production of artefact	✓
Reflective log/diary	✓	Practice file	✓

Indicative Content

This content serves as guidance and illustrative examples rather than a prescribed or exhaustive set of requirements

Learning Outcome 1 – Understand how cyber threats affect individuals and organisations:

Delivery could include exploring types of threats such as phishing, data theft, social engineering, malware or weak passwords, how they affect individuals by losing access or privacy, and how they affect organisations through disruption, cost or reputational harm, as well as explaining how cyber security supports safe digital behaviour by encouraging awareness, responsible access and checking.

Learning Outcome 2 – Know how to choose appropriate cyber-safe actions for different situations:

Learners could compare threats such as phishing versus malware or personal versus organisational risk, consider factors like urgency, reliability and seriousness when choosing a response, and explore how to check whether a response worked by reviewing outcome, checking feedback, monitoring behaviour or confirming access remains safe.

Learning Outcome 3 – Be able to apply cyber safe practices to complete a task:

Delivery could involve applying cyber-safe practices to a purposeful task such as handling information securely, assessing a potentially risky message, updating account settings appropriately or responding to a simulated incident, applying responsible behaviours including evaluating risks before acting,

selecting appropriate actions, checking the accuracy and impact of what they have done, and reviewing effectiveness to identify strengths, limitations and how practice could be improved.