

Online Safety

Entry Level 1 – Level 2

Skills for Life and Work
Unit Specification

Contents

Unit Aim.....	3
Units from Other Awarding Organisations	3
Qualification Documentation	3
Progression Across Levels	4
Delivery Requirements	6
Assessment Approach.....	8
Entry Level 1.....	8
Entry Level 2.....	9
Entry Level 3.....	10
Level 1	11
Level 2.....	12
Unit Content	13
Entry level 1	13
Entry level 2.....	16
Entry level 3.....	19
Level 1	22
Level 2.....	25

Unit Aim

This unit is part of the Skills for Life, Skills for Work, and Skills for Life and Work qualifications, available at Entry Level 1–3, Level 1 and Level 2 to support the 14-16 Curriculum for Wales.

The 'Online Safety' suite of units has been designed to develop Learners' knowledge of online safety and the nature of possible threats that they could encounter while engaging in activity through the internet and the skills to protect themselves and others from harm, including knowing when to ask for support and when to report unsafe activity.

Units from Other Awarding Organisations

Only units that form part of the approved Open Awards Skills for Life, Skills for Work, and Skills for Life and Work qualifications may contribute towards achievement of this qualification.

Units certificated by other Awarding Organisations, or units taken from other Open Awards qualifications, cannot contribute to the achievement of this qualification. This requirement applies across all levels and qualification sizes.

Qualification Documentation

This Unit Specification is a mandatory document and must be read and applied alongside the relevant Qualification Guide (level-specific) and the Open Awards Provider Handbook.

Progression Across Levels

This suite of units has been designed for learners ranging from Entry Level 1 – Level 2. Learners may progress through the levels throughout their education journey or start at a higher level as appropriate to their level of learning, education targets and aspirations.

The table below summarises the areas of learning included within the units and how these are treated at each level.

Concept	Entry 1	Entry 2	Entry 3	Level 1	Level 2
Understanding online activity	Identify everyday online activities	Identify safe online behaviours	Understand safe behaviour across tasks	Explain safe practices in different contexts	Assess effectiveness of safety practices
Staying safe online	Recognise ways to stay safe	Identify and demonstrate safe behaviours	Apply safety behaviours in familiar and unfamiliar tasks	Apply and review safe practices	Adapt safety practices to changing situations
Online risks and threats	Recognise unsafe behaviour	Identify unsafe online activities	Understand types of online risks	Explain online threats and unsafe behaviour	Analyse threats and judge levels of risk
Responding to online situations	Demonstrate simple responses	Demonstrate actions when unsure	Apply strategies to manage risks	Apply strategies to manage risks in context	Select and justify responses to complex risks
Seeking help and reporting	Identify trusted individuals	Identify when and who to seek help from	Identify situations requiring reporting	Describe when and how to report concerns	Evaluate reporting decisions and methods

Communication and reflection	State simple responses	Give examples of actions	Describe actions and outcomes	Review own behaviour	Evaluate and justify decisions
Cognitive demand	Recognise / identify	Identify / give examples / demonstrate	Describe / apply	Explain / apply / review	Analyse / evaluate / justify / adapt

Delivery Requirements

Before delivery, providers must have an approved Delivery and Assessment Plan that maps teaching, learning and assessment to all (level-specific) assessment criteria in this Unit Specification.

Providers are expected to plan and deliver learning and assessment activities within standard school/college/training provider facilities. This unit should be accessible and deliverable without requiring specialist infrastructure, high-cost resources or restrictive entry conditions.

Staffing Resources

Providers must ensure suitably qualified and experienced teachers are available to deliver and assess this unit.

Delivery staff must:

- have knowledge and understanding of online safety, including digital risks, safe behaviours, and reporting procedures appropriate to the level of delivery
- be able to support learners in developing safe and responsible use of online technologies
- understand safeguarding requirements and know how to respond appropriately to learner disclosures or concerns

Delivery should be supported by:

- staff who can facilitate discussion of sensitive topics (e.g., online harm, cyberbullying, inappropriate content) in a safe and supportive manner
- staff who can model safe digital behaviour and promote responsible online decision-making
- access to pastoral or safeguarding support where required.

Delivery staff should hold, or be working towards, a recognised teaching or training qualification where this is a requirement of the provider.

Physical Resources

Providers must ensure suitable and sufficient resources are available to deliver and assess this unit.

As a minimum this should include:

Learning Environment

- a safe and inclusive learning environment that supports discussion of online behaviour and digital safety
- access to a controlled digital environment where learners can practise online skills safely.

Teaching and Learning Materials

- structured lesson plans and session materials to support consistent delivery
- learner handouts and activity materials to support understanding and application of online safety concepts
- scenario-based materials and case studies to explore online risks and appropriate responses
- visual resources such as diagrams, prompts, and examples of online interfaces.

Equipment

- access to digital devices, e.g., computers, laptops, or tablets
- reliable internet access with appropriate filtering and safeguarding measures in place
- presentation equipment, e.g., projector or interactive screen
- classroom resources including whiteboard and writing materials.

Entry Requirements

Learners do not require any prior learning or qualifications for any of the units within this suite. However, as the level of complexity of language increased through the levels, the provider must complete robust initial assessments to ensure the learner is able to access the content at the level they are starting.

Assessment Approach

This suite of units has been designed to be assessed through assessment tasks and activities designed by the provider.

Providers must undertake pre-course verification prior to assessment taking place to confirm tasks cover all assessment criteria and are appropriate to the level.

All assessment criteria must be met in full for the learner to be awarded a 'pass'. No partial award can be made if any assessment criteria is not met.

Learners are required to collate evidence in a portfolio. This can be presented digitally (e.g., through an e-portfolio system) or as paper-based as appropriate to the individual learner. Wherever possible, e-portfolios are encouraged.

Assessors must assess the evidence collated by the learner against the assessment criteria within the unit to determine whether each has been met in full or not. All assessment decisions are subject to internal quality assurance (IQA) by the provider and external quality assurance (EQA) by Open Awards before the result is confirmed.

The following types of assessment tasks have been determined to be suitable for this unit at each level.

Entry Level 1

Assessment of Online Safety at Entry Level 1 should include:

Assessment Type	Examples of Tasks
Matching / Sorting	Learners match online activities (e.g., games, videos) to images or labels.
Identification Task	Learners identify safe and unsafe online behaviours from pictures or scenarios.
Pointing / Selecting	Learners identify ways to stay safe online (e.g., not sharing personal details).
Demonstration	Learners demonstrate a simple safety action (e.g., logging out, asking for help).
Scenario Task (Supported)	Learners respond to simple online scenarios (safe/unsafe).
Verbal Response	Learners state what they use the internet for.
Practical Activity	Learners create a list or visual of trusted individuals.

Entry Level 2

Assessment of Online Safety at Entry Level 2 should include:

Assessment Type	Examples of Tasks
Matching / Sorting	Learners match safe and unsafe online behaviours to given scenarios.
Identification Task	Learners identify strategies to stay safe online.
Demonstration	Learners demonstrate safe use of devices (e.g., logging out, recognising secure symbols).
Practical Task	Learners complete a simple online activity following safety instructions.
Scenario-Based Task	Learners select appropriate responses to unsafe situations.
Short Verbal / Written Response	Learners give examples of when to seek help.
Practical Activity	Learners create a list of trusted individuals across contexts.

Entry Level 3

Assessment of Online Safety at Entry Level 3 should include:

Assessment Type	Examples of Tasks
Short Written / Oral Task	Learners outline safe online behaviours and describe strategies.
Scenario Analysis	Learners identify unsafe behaviours and associated risks.
Demonstration	Learners demonstrate safe behaviour during online tasks.
Practical Task	Learners complete unfamiliar tasks following safety instructions.
Identification Task	Learners identify risks such as scams, bullying, or data sharing.
Reporting Task	Learners identify situations that should be reported and to whom to report to.
Reflection Task	Learners reflect on how their actions impact safety.

Level 1

Assessment of Online Safety at Level 1 should include:

Assessment Type	Examples of Tasks
Written / Oral Task	Learners explain safe practices across different online activities.
Scenario Task	Learners describe ways to manage online risks in given situations.
Demonstration	Learners demonstrate safe behaviour across a range of online tasks.
Reflection Task	Learners review their own online behaviour and identify improvements.
Research Task	Learners outline types of online threats.
Explanation Task	Learners explain why certain behaviours are unsafe.
Scenario-Based Task	Learners describe situations requiring reporting.
Practical Task	Learners demonstrate use of reporting tools or processes.

Level 2

Assessment of Online Safety at Level 2 should include:

Assessment Type	Examples of Tasks
Analytical Task	Learners assess effectiveness of safety measures in different scenarios.
Scenario-Based Task	Learners explain appropriate safety actions for complex situations.
Demonstration	Learners complete multi-step online tasks using safe practices.
Adaptation Task	Learners respond to emerging risks during a task.
Research Task	Learners analyse online threats and their impact.
Discussion / Written Task	Learners justify levels of risk in different scenarios.
Evaluation Task	Learners evaluate when reporting is required.
Practical Task	Learners select and use appropriate reporting methods with justification.

Unit Content

Entry Level 1

Unit Title: Online Safety

Unit Reference Number: CBM116

Level: Entry Level One (1)

Credit Value: Two (2)

Guided Learning Hours: 20

Unit Aim: To develop Learners' knowledge of online safety and the nature of possible threats that they could encounter while engaging in activity through the internet and the skills to protect themselves and others from harm, including knowing when to ask for support and when to report unsafe activity.

Principles of Progression

Progression 1 - I can identify who looks after me and who my family and friends are.

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Know everyday online activities	1.1 Identify everyday online activities
	1.2 State what they use the internet for
2. Know ways to stay safe online	2.1 Identify ways to stay safe online
	2.2 Demonstrate a way to stay safe online
3. Know unsafe online behaviour	3.1 Identify examples of unsafe online behaviour
	3.2 Demonstrate what to do if unsure online
4. Know who to go to for help online	4.1 Identify trusted individuals
	4.2 Identify when to ask for help

Indicative Content

LO1 AC 1.1 Learners must state or identify, using visuals, at least one everyday online activity e.g.,

- watching videos
- playing games
- contacting friends and family.

AC 1.2 Learners must state or select from a range of visuals at least one online activity that they regularly participate in e.g.,

- watching videos
- playing games
- contacting friends and family.

LO2 AC 2.1 Learners must state or identify, using visuals, at least two ways to stay safe online e.g.,

- hiding passwords
- asking before opening an app
- logging out of accounts.

AC 2.2 Learners must demonstrate at least one way of staying safe online e.g.,

- logging out of an account
- checking with a tutor before opening an app/attachment.

LO3 AC 3.1 Learners must state or identify at least two unsafe online activities e.g.,

- speaking to strangers
- sharing personal details
- posting photos without people knowing.

AC 3.2 Learners must demonstrate at least one simple practical action to take if they are unsure or worried about something online e.g.,

- seeking out a trusted individual
- not clicking a link
- using a report/ block button with support.

LO4 AC 4.1 Learners must identify at least two examples.

AC 4.2 Learners must accurately respond to at least two scenarios, identifying whether it is safe or they need to get help e.g.,

- 'A message from someone you don't know'
- 'Playing a game with a good friend from school'

Area of Learning Experience	Health and wellbeing
Statement of What Matters	Healthy relationships are fundamental to our well-being.
Links to the Four Purposes	Purpose 4 - Healthy, confident individuals, ready to lead fulfilling lives as valued members of society
Cross-curricular Skills	Literacy and Digital
Integral Skills	Personal effectiveness
Understanding of sustainability in the world of work and/or everyday work	Using online tools and applications safely support long-term wellbeing and ethical, sustainable choices in everyday life.

Relevant Cross-Cutting Themes	
Theme	Rationale
Human rights	Addresses digital safety and protection.

Entry Level 2

Unit Title: Online Safety

Unit Reference Number: CBM117

Level: Entry Level Two (2)

Credit Value: Two (2)

Guided Learning Hours: 20

Unit Aim: To develop Learners' knowledge of online safety and the nature of possible threats that they could encounter while engaging in activity through the internet and the skills to protect themselves and others from harm, including knowing when to ask for support and when to report unsafe activity.

Principles of Progression

Progression step 2 - I can recognise that there are different types of relationships beyond my family and friends.

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Know ways to stay safe online	1.1 Give examples of online activities
	1.2 Identify ways to stay safe when online
2. Be able to use online devices safely	2.1 Demonstrate how to stay safe when using devices
	2.2 Follow instructions to stay safe online
3. Know unsafe online behaviour	3.1 Identify unsafe online activities
	3.2 Demonstrate actions to take if unsure online
4. Understand when to seek help online	4.1 Identify trusted individuals in different contexts
	4.2 Give examples of when to seek help

Indicative Content

LO1 AC 1.1 learners must give at least two examples of online activities that they might participate in e.g.,

- Talking to friends through a social media application
- Posting pictures on social media
- Playing video games
- Shopping online
- Planning a trip

AC 1.2 Learners must identify at least two ways to stay safe online e.g.,

- include hiding passwords
- asking before opening an app
- logging out of accounts.

LO2 AC 2.1 Learners must demonstrate using at least two devices safely e.g.,

- logging out of an account on a laptop
- checking a padlock symbol on a phone.

AC 2.2 Learners must complete a short online task following simple verbal or written safety instructions e.g.,

- opening a new education app or website
- using only the details given
- not entering personal details and safely storing a password.

LO3 AC 3.1 Learners must identify at least two unsafe online activities e.g.,

- talking to strangers in an application
- sharing personal details in a social media

AC 3.2 Learners must demonstrate at least two simple practical actions to take if they are uncertain about online activities e.g.,

- seeking out a trusted individual
- not clicking a link
- using a report / block button with support.

LO4 AC 4.1 Learners must identify examples from at least two different contexts e.g.,

- home
- school
- community and social settings relevant to them.

AC 4.2 Learners must identify at least two examples.

Area of Learning Experience	Health and Wellbeing
Statement of What Matters	Healthy relationships are fundamental to our well-being.
Links to the Four Purposes	Purpose 4 - Healthy, confident individuals, ready to lead fulfilling lives as valued members of society
Cross-curricular Skills	Literacy and Digital
Integral Skills	Personal effectiveness
Understanding of sustainability in the world of work and/or everyday work	Using online tools and applications safely support long-term wellbeing and ethical, sustainable choices in everyday life.

Relevant Cross-Cutting Themes	
Theme	Rationale
Human rights	Addresses digital safety and protection.

Entry Level 3

Unit Title: Online safety

Unit Reference Number: CBM118

Level: Entry Level Three (3)

Credit Value: Two (2)

Guided Learning Hours: 20

Unit Aim: To develop Learners' knowledge of online safety and the nature of possible threats that they could encounter while engaging in activity through the internet and the skills to protect themselves and others from harm, including knowing when to ask for support and when to report unsafe activity.

Principles of Progression

Progression step 3 - I can understand that there are differences within types of relationships and that relationships change over time.

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Understand safe online behaviour	1.1 Outline safe behaviours for online tasks
	1.2 Describe ways to stay safe in unfamiliar online situations
2. Be able to apply online safety skills	2.1 Demonstrate safe behaviour during online tasks
3. Understand online risks	3.1 Identify unsafe online behaviour and risks
	3.2 Identify how online actions can cause harm
4. Understand reporting online concerns	4.1 Give examples of situations that should be reported
	4.2 Identify appropriate people and services to report concerns to

Indicative Content

LO1 AC 1.1 Learners must outline at least three safe online behaviours for familiar tasks.

AC 1.2 Learners must describe three routine ways to stay safe online, which can be applied to unfamiliar tasks.

LO2 AC 2.1 Learners must demonstrate at least three ways of staying safe online e.g.,

- logging out of an account
- checking with a tutor before opening an app/attachment
- logging out of a shared device.

LO3 AC 3.1 Learners must identify at least three examples of unsafe behaviour across a range of scenarios, identifying the type of risk e.g.,

- bullying
- scams
- requests for personal information.

AC 3.2 Learners must identify at least three online actions that could cause harm, with a basic reason e.g., posting something that reveals an individual's location makes it easier for a stranger to find them.

LO4 AC 4.1 Learners must select at least three examples of online behaviour that should be reported across a range of scenarios e.g.,

- threats
- bullying
- requests for data and suspicious messages.

AC 4.2 Learners must state two familiar trusted individuals and two services to whom they can report concerns.

Area of Learning Experience	Health and Wellbeing
Statement of What Matters	Healthy relationships are fundamental to our well-being.
Links to the Four Purposes	Purpose 4 - Healthy, confident individuals, ready to lead fulfilling lives as valued members of society
Cross-curricular Skills	Literacy and Digital
Integral Skills	Personal effectiveness
Understanding of sustainability in the world of work and/or everyday work	Using online tools and applications safely support long-term wellbeing and ethical, sustainable choices in everyday life.

Relevant Cross-Cutting Themes	
Theme	Rationale
Human rights	Addresses digital safety and protection.

Level 1

Unit Title: Online Safety

Unit Reference Number: CBM119

Level: One (1)

Credit Value: Two (2)

Guided Learning Hours: 20

Unit Aim: To develop Learners' knowledge of online safety and the nature of possible threats that they could encounter while engaging in activity through the internet and the skills to protect themselves and others from harm, including knowing when to ask for support and when to report unsafe activities.

Principles of Progression

Progression step 4 - I can show a developing awareness of the complex nature of relationships.

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Understand safe online behaviour	1.1 Describe ways to manage risks in different online situations
2. Be able to apply online safety skills	2.1 Demonstrate safe behaviour during online tasks
	2.2 Follow safety instructions when completing unfamiliar tasks
3. Understand online risks	3.1 Identify unsafe online behaviour and the associated risks
	3.2 Identify how online actions can cause harm
	3.3 Risk assess own behaviours when completing online tasks
4. Understand reporting online concerns	4.1 Outline situations that should be reported
	4.2 Demonstrate using appropriate methods to report concerns

Indicative Content

- LO1 AC 1.1 Learners must describe at least four ways to manage risks when engaging with online content e.g.,
- avoiding fake websites by checking information sources
 - using antivirus software to protect against malware
 - avoid clicking unknown links or opening attachments from unknown sources.

- LO2 AC 2.1 Learners must demonstrate safe behaviours across a range of real and simulated activities e.g.,
- browsing
 - downloading
 - gaming
 - using social media.

AC 2.2 Learners must demonstrate following instructions for at least three unfamiliar online activities e.g.,

- installing software
- online shopping
- using antivirus software.

- LO3 AC 3.1 Learners must identify types of online threats and associated risks showing how to manage them e.g.,

- phishing
- malware
- impersonation.

AC 3.2 Learners must identify at least three examples of unsafe behaviours and the harm they could cause e.g.,

- sharing too much personal information which could lead to identity theft
- posting inappropriate content, which might damage a person's reputation

AC 3.2 Learners must carry out an assessment of their own online safety practices. They should create up to three personal targets for safe online use. Including:

- what they do well
- what issues they face
- their current confidence level to deal with challenges
- areas for improvement.

LO4 AC 4.1 Learners must outline at least three situations that need to be reported, using examples e.g.,

- cyberbullying with examples
- scam attempts with details of how these can appear
- inappropriate and harmful content, with examples.

AC 4.2 Learners must use two agreed methods to report concerns e.g.,

- using a report button in an email
- sending an email to a tutor.

Area of Learning Experience	Health and Wellbeing
Statement of What Matters	Healthy relationships are fundamental to our well-being.
Links to the Four Purposes	Purpose 4 - Healthy, confident individuals, ready to lead fulfilling lives as valued members of society
Cross-curricular Skills	Literacy and Digital
Integral Skills	Personal effectiveness
Understanding of sustainability in the world of work and/or everyday work	Using online tools and applications safely support long-term wellbeing and ethical, sustainable choices in everyday life.

Relevant Cross-Cutting Themes

Theme	Rationale
Human rights	Addresses digital safety and protection.

Level 2

Unit Title: Online Safety

Unit Reference Number: CBM1201

Level: Two (2)

Credit Value: Two (2)

Guided Learning Hours: 20

Unit Aim: To develop Learners' knowledge of online safety and the nature of possible threats that they could encounter while engaging in activity through the internet and the skills to protect themselves and others from harm, including knowing when to ask for support and when to report unsafe activity.

Principles of Progression

Progression step 5 - I can show an understanding of the complex nature of relationships in a range of contexts and an understanding of how they are influenced by a range of factors

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Understand online safety measures	1.1 Assess the effectiveness of online safety measures in different contexts
2. Be able to apply and adapt online safety practices	2.1 Demonstrate applying online safety practices
	2.2 Adapt behaviour in response to emerging risks
3. Understand online threats	3.1 Analyse online threats and their impact
	3.2 Assess levels of risk in online scenarios
4. Know how to use appropriate reporting procedures	4.1 Describe when reporting is necessary
	4.2 Describe the appropriate reporting procedures

Indicative Content

LO1 AC 1.1 Learners must assess the effectiveness of online safety measures and actions in at least three different complex contexts. They must explain their reasoning e.g.,

- coming across a fake website when shopping online
- receiving an email from an unknown sender when at work.

LO2 AC 2.1 Learners must carry out a simulated multi-step online task to show how they would apply online safety practices. Learners must explain the safety measures they have taken to keep themselves safe online.

Example:

- researching a topic and creating a presentation
- registering with and carrying out an online shop.

AC 2.2 Learners must respond to identified risks whilst completing the activity in AC 2.1 explaining their decisions e.g.,

- using a different website as they identified it was not a secure site
- choosing not to sign up to a mailing list to access materials because it asked for personal details

LO3 AC 3.1 Learners must analyse at least three online threats, including the potential impact.

AC 3.2 Learners must assess the level of risk for at least three given scenarios.

LO4 AC 4.1 Learners must describe when reporting is necessary across a range of different online scenarios, commenting on severity, urgency, potential impact, and personal responsibility.

AC 4.2 Learners must select and explain the appropriate reporting mechanism for each online scenario in AC 4.1.

Area of Learning Experience	Health and Wellbeing
Statement of What Matters	Healthy relationships are fundamental to our well-being.
Links to the Four Purposes	Purpose 4 - Healthy, confident individuals, ready to lead fulfilling lives as valued members of society
Cross-curricular Skills	Literacy and Digital
Integral Skills	Personal effectiveness
Understanding of sustainability in the world of work and/or everyday work	Using online tools and applications safely support long-term wellbeing and ethical, sustainable choices in everyday life.

Relevant Cross-Cutting Themes	
Theme	Rationale
Human rights	Addresses digital safety and protection.