

Online safety

Unit delivery and assessment pack



Made for Wales.
Ready for the world.

Contents

This unit delivery and assessment pack provides teachers with the information they need to deliver this unit.

The pack is structured as follows:

Unit overview	3
Entry Level Learning Outcomes and Assessment Criteria	5
Level 1 and Level 2 Learning Outcomes and Assessment Criteria	7
Delivery guidance	9
Planning courses	9
Amplification of Learning Outcomes	9
Suggested activities.....	12
Sources of evidence	13
Experiences.....	13
Resources and organisations	14
Resources required for delivery	14
Resources available to support delivery	14
Resources required for assessment.....	15

The UK Government has announced plans to restrict social media use by children under 16, which may impact some of our qualifications. We will keep our qualifications under review and make any necessary updates as further details become available

Unit overview

Title	Online safety
Suite	Skills for Life
Unit Codes	S620E1 S620E2 S620E3 S620L1 S620L2
GLH	20
Unit Aim	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.
Unit Summary	This unit helps learners understand the importance of staying safe online and how to protect themselves and others when using the internet. Learners will explore common online threats, such as scams, cyberbullying, and unsafe communication, and learn how to behave responsibly in digital spaces. They will also find out who they can go to for help and how to report anything that makes them feel uncomfortable or unsafe. The unit builds confidence in recognising risks, acting safely, and knowing how to get support if needed.
Curriculum for Wales	Areas of learning: This unit supports progress towards the following Health and well-being statements of what matters: <i>How we process and respond to our experiences affects our mental health and emotional wellbeing</i>, <i>How we engage with social influences shapes who we are and affects our health and wellbeing</i>, and <i>Our decision-making impacts on the quality of our lives and the lives of others</i>. When exploring online safety, learners will identify and respond to different online situations, recognise how their actions and interactions can affect their own and others' wellbeing, and, as appropriate to their level, demonstrate safe, respectful, and responsible behaviours when engaging online. Integral and cross-curricular skills: Learners will have opportunities to develop their Digital competency through planning digital work and creating formal text documents using digital tools to enhance and refine their work. Learners will also demonstrate their Literacy skills by responding to online risks, using discipline-specific vocabulary, and reading and researching a range of texts and sources to develop understanding of a topic. Cross-cutting themes: Relationships and sexuality education (RSE) Learners develop their awareness of respectful and safe behaviour online, and how to respond to inappropriate or harmful contact.

Human rights

Learners will learn about different risks, including online abuse, hate speech, misinformation, and bias, and learn to promote inclusion, tolerance, and digital citizenship.

Careers and work-related experiences

Learners develop an understanding of how online behaviour can affect future education or employment opportunities.

Entry Level Learning Outcomes and Assessment Criteria

Learning Outcomes (the learner will)	Assessment criteria (the learner can)		
	Entry 1	Entry 2	Entry 3
LO1 Know what online safety means and why it is important	E1 1.1 Identify (from a set of examples) what online safety is. E1 1.2 Give one simple reason why online safety is important.	E2 1.1 Give a statement about what online safety means. E2 1.2 Give at least two reasons why keeping safe online is important.	E3 1.1 Give a description of what online safety means. E3 1.2 Explain why it is important to stay safe when using the internet.
LO2 Know about different types of online risks and unsafe behaviour	E1 2.1 Point out an example of an online risk. E1 2.2 Point out an example of unsafe behaviour.	E2 2.1 Recognise a type of online risk. E2 2.2 Recognise a type of unsafe behaviour. E2 2.3 Indicate why the risk or behaviour can be harmful.	E3 2.1 Give examples of different types of online risks. E3 2.2 Give examples of different types of unsafe behaviour. E3 2.3 Explain how these risks and behaviours could affect people.
LO3 Be able to stay safe when online	E1 3.1 Follow simple steps to stay safe when using the internet. E1 3.2 Show how to keep personal information private (with support).	E2 3.1 Show two examples of safe online behaviour. E2 3.2 Carry out safe actions to protect personal information. E2 3.3 Follow instructions to use privacy settings when online.	E3 3.1 Use different ways of staying safe when online. E3 3.2 Demonstrate simple steps to protect personal information and devices from harm. E3 3.3 Use privacy settings to control who can see personal information when online.

LO4 Know how and when to get help, and report unsafe activity online	E1 4.1 Point out someone who can help with online safety. E1 4.2 Name a type of unsafe online activity that should be reported.	E2 4.1 Recognise when someone should ask for help with online safety. E2 4.2 Give an example of a person or organisation who can help with online safety. E2 4.3 State how to report unsafe online activity.	E3 4.1 Describe how and when to ask for help or report concerns about online safety. E3 4.2 Give examples of people or organisations who can help with online safety and state how they can help. E3 4.3 Explain why it is important to report unsafe or worrying online behaviour.
--	---	--	---

If not specified, then a plural reference within assessment criterion refers to a minimum of two.

Level 1 and Level 2 Learning Outcomes and Assessment Criteria

Learning Outcomes (the learner will)	Assessment criteria (the learner can)	
	Level 1	Level 2
LO1 Know what online safety means and why it is important in different contexts	L1 1.1 Describe what online safety means. L1 1.2 Explain several reasons why online safety is important. L1 1.3 State the purpose of the Children's Code.	L2 1.1 Describe what online safety means in different contexts. L2 1.2 Explain why protecting personal data and privacy online is important. L2 1.4 Describe how the Children's Code helps protect children online.
LO2 Be able to recognise different online risks and unsafe behaviour	L1 2.1 Identify different types of online risks. L1 2.2 Identify some examples of unsafe online behaviour. L1 2.3 Give examples of how these risks or behaviours can be harmful. L1 2.4 Show how suspicious or harmful online activities can be recognised.	L2 2.1 Identify and explain different types of online risks and why they are harmful. L2 2.2 Recognise different types of unsafe behaviour and explain their potential consequences. L2 2.3 Demonstrate how to recognise suspicious or harmful online activity.
LO3 Be able to demonstrate safe online practices and explain why they are important	L1 3.1 Apply safe practices when using the internet. L1 3.2 Demonstrate a range of ways to protect personal information online. L1 3.3 Describe why it is important to follow safe online practices.	L2 3.1 Demonstrate safe online practices in different online contexts. L2 3.2 Explain why each practice helps to protect personal safety and privacy. L2 3.3 Give examples of situations where safe online practices prevent harm or reduce risks.

LO4 Know how and when to get help and report unsafe activity online	L1 4.1 Suggest when it is necessary to get help or report unsafe online activities. L1 4.2 Identify who to ask for help if something unsafe happens online. L1 4.3 Identify ways to report unsafe activity online.	L2 4.1 Explain when it is necessary to get help or report unsafe activity online. L2 4.2 Identify sources of help or advice for unsafe activity online and how they can help. L2.4.3 Explain different ways to report unsafe activity and the potential outcomes.
---	--	---

If not specified, then a plural reference within assessment criterion refers to a minimum of two.

Delivery guidance

Planning courses

Each unit in the Skills for Life and Work suite is awarded individually. When planning courses, teachers should consider the potential qualification outcomes for individual learners.

Closely related units that might be delivered alongside Online safety include Science and technology in everyday life, Digital film and media, Mental health and wellbeing, Personal safety, and Using IT in the workplace. These units complement each other as they support understanding of how technology works and how to use it safely and responsibly, how online activity can affect emotions and how to manage risks like cyber bullying and also by promoting awareness of how to stay safe both online and offline.

There may also be links to other WJEC qualifications including an Award in Internet Safety for IT Users and Keeping Safe Online as part of WJEC's Post 16 Pathways to Employment qualification, the Level 1/2 Vocational Award in ICT, and the General Foundation Qualification in Digital Technology.

For full details of the Skills for Life and Work units and qualifications please refer to the qualification specification.

Amplification of Learning Outcomes

The amplification of the learning outcomes provided below should support teachers in developing content for delivery. Teachers can develop and tailor content as appropriate to their learners, whilst ensuring that the learners are providing with knowledge, understanding and the opportunity to develop and apply the skills needed to meet the learning outcomes and assessment criteria. Content should be considered in the context of:

- the level the learner is working at
- providing opportunities for progression
- centre facilities and resources
- local, national and international contexts as appropriate.

Teachers may find it helpful to refer to the level descriptors within the qualification specification.

Learning outcome	Amplification
LO1	What online safety means: • keeping information and devices safe when using the internet • protecting individuals and data. Types of contexts: • social media • email • gaming • online shopping.

	For Level 1 and 2 learners: • Important because it: • prevents identity theft • keeps people safe from harm and exploitation • The Children's Code's purpose: • ensures apps and websites protect young people's privacy.
LO2	Online threats/risks: • unwanted messages from strangers • unkind or hurtful messages online (cyberbullying) • fake friend requests or fake social media profiles • harmful content (e.g. content that promotes harmful behaviour) • pop-up adverts or links that look suspicious • personal data risks (e.g. misuse or exploitation of personal data) • unsafe websites pretending to be real ones. Unsafe behaviour/activity: • sharing personal information (e.g. name, address, school, phone number) online • sharing images of ourselves and others online • using weak passwords or sharing passwords • clicking on unknown or suspicious links • accepting friend requests from strangers • posting offensive or unkind comments • downloading files from unknown sources • sharing location. For Level 1 and 2 Learners: Online threats/risks: • viruses, malware, or phishing scams that steal data or damage devices • hacking or identity theft • online scams and fraud (e.g. fake competitions, investment or delivery scams) • cyberbullying from harassment, or trolling • fake websites, adverts, or social media profiles designed to mislead users • unsafe contact from strangers (e.g. grooming or exploitation attempts) • content that could indicate radicalisation, exploitation or abuse • oversharing or weak privacy settings leading to data misuse.

LO3	Stay safe by: • using a strong password • not sharing passwords • checking before sharing personal information • recognising safe/unsafe websites • avoiding suspicious links/emails • updating device software • reporting abuse. Protect personal information by: • logging off • not sharing personal details and passwords • blocking users • saving evidence • using privacy settings on social media • changing social media profile to private • adjusting app permissions or parental controls. For Level 1 and 2 Learners: Safe online practices could include: • applying safe practices in different online contexts (social media, email, online shopping, gaming) • recognising and avoiding suspicious links, messages, or emails • updating device software and apps • reporting unsafe or concerning activity. Strategies to protect personal information and privacy could include: • using privacy settings and strong passwords to protect accounts • logging off and securing accounts when not in use • blocking or reporting unsafe contacts • controlling who can see personal information or posts.
LO4	Get help when something online is: • unsafe • worrying • wrong. Unsafe activity to report: • bullying, rude threatening messages • friend requests or messages from strangers • inappropriate or harmful content • fake profiles or scam messages • suspicious links or files. Get help by telling a: • parent • teacher • trusted adult

	• using 'Report' button'. For Level 1 and 2 Learners: Report unsafe behaviour by: • using reporting tools on websites, games and social media • reporting to platform moderators • saving evidence to support report (e.g. screenshots, notes, recordings). Organisations that can help: • CEOP • Childline • The UK Safer Internet Centre.
--	--

Suggested activities

This section gives some suggested activities to support teaching and learning in a vocational context consistent with the philosophy and intent of the unit and associated qualifications. Useful resources and possible contacts that could be made in the delivery of the learning are also signposted.

The following activities would be suitable for use with Entry Level learners:

- group discussion: "What is online safety?"
- tick-box or card sort: identify safe vs unsafe behaviour (show fake messages, friend requests, pop-up adverts)
- matching/sorting activity: sorting unsafe situations to the correct response
- observation of online activity: demonstrating safe searches or checking websites
- role-play: practising simple safe actions (e.g., not sharing personal information) or responding to unsafe situations ("Who would you tell?") role-play: simulating being asked for personal information in a shop (e.g. name, address, PIN, or card details); discussing safe responses and linking this to online safety (e.g., not sharing passwords or full name)
- tick-box: select correct reporting options.

The following activities would be suitable for use with Level 1 and 2 learners:

- worksheet/card sort: threats to online safety – types of online risks and unsafe behaviours (e.g., phishing, cyberbullying)
- quiz: true/false or matching safe behaviours
- group discussion on why staying safe online is important
- poster or presentation - explaining online safety and safe practices in different contexts (e.g. demonstrating safe actions like using strong passwords, secure sites, privacy settings) and why they matter
- case study analysis of consequences of unsafe behaviour or model safer alternatives and justify choices
- class discussion on the Children's Code or the potential consequences of unsafe online behaviour
- scenario-based quiz/response exercise: "What would you do if...?" (e.g. suspicious links, cyberbullying, phishing)
- case studies: identify unsafe actions, explain risks, model safer alternatives
- scenario-based role-play: practice responding safely to unsafe situations

- creating a personal online safety plan: protecting personal data, adjusting privacy settings, responding to unsafe situations, reporting concerns
- detailed poster, guide, or presentation: explain safe practices and why they matter
- worksheet or card sort: sources of help and how they can support users
- scenario-based task: decide when and how to report unsafe activity (e.g. cyberbullying, suspicious messages, or unsafe content) and explain why reporting is necessary
- group discussion and presentation: explain different reporting methods and potential outcomes
- scenario/discussion: considering Prevent and Safeguarding - discussing how trusted adults respond if someone reports unsafe or concerning online activity.

Sources of evidence

This unit is centre assessed and externally quality assured by WJEC. Assessment must be accessible, using clear language and reflecting the learner's level. Learners should demonstrate knowledge and skills through realistic activities such as roleplay, case studies, or projects. Whilst evidence may be verbal, written, practical or visual, extended written work is not required unless appropriate. Each unit must be assessed independently, even if tasks cover multiple criteria. Assessor judgements should focus on the meeting of standards, not on spelling or presentation unless specifically assessed. Full assessment guidance is available in the qualification specification.

Possible sources of evidence may include:

- Completed tick-box or matching worksheet
- Quiz responses
- Notes or summaries from group discussions
- Digital or paper posters for online practices
- Written or typed explanations of scenario responses
- Completed worksheets for sources of help
- Annotated screenshots showing safe responses
- Audio or video description of actions taken in scenario tasks
- Slide deck, infographic or one-page help sheet
- Voice-over video or screen-recorded explanations
- Completed case studies
- Video or audio recording of presentation
- Screen recording of a narrated presentation (e.g. PowerPoint or Sway)
- Written plan or digital checklist of safety plan
- Flowchart or mind map
- Video or audio reflection
- Written reflections or explanations of reporting methods
- Teacher observation notes or checklist.

Experiences

To provide a real-world context you could invite:

- a local school IT technician or e-safety officer to provide anonymised examples of real incidents at the school or local community (e.g., phishing emails, cyberbullying, inappropriate app usage). Working in groups, learners could analyse the incidents, identify risks, and decide how to respond safely according to best practices. The technician can then explain the actual outcomes and safety measures used, reinforcing the importance of reporting, safe passwords, and privacy settings.

- a social media manager or digital marketing professional to explain how they manage accounts safely online, including setting privacy settings, monitoring comments, and reporting inappropriate content. Learners could be given a scenario of a small business social media page with potential risks (e.g., spam messages, inappropriate comments, phishing attempts). Learners could identify risks, suggest safe responses (blocking users, reporting abuse, adjusting privacy settings), and present their safety plan to the professional. The professional can then share how they handle these situations in practice, highlighting challenges such as managing multiple platforms or preventing data breaches.
- a cybersecurity professional or ethical hacker. Learners could be given a simplified case study of a business or individual whose online accounts were compromised and could use mock tools or worksheets to identify vulnerabilities, suggest safe online practices, and create a short action plan for prevention. The professional could then explain how real businesses protect data, manage risks, and respond to breaches, showing how online safety practices are applied in professional contexts.

Resources and organisations

Resources required for delivery

This unit has been designed to be delivered using standard classroom environments, supported by access to appropriate practical spaces, when demonstrations are required, and commonly available resources.

Resources available to support delivery

Digital Communities Wales	Offers online resources that focus on case studies and digital inclusion provides a resource library on digital inclusion. To find out more, go to https://www.digitalcommunities.gov.wales/resources/
Cwmpas	Provides a resource that focuses on identifying misinformation and disinformation, developing media literacy, and identifying online bias. To find out more, go to https://cwmpas.coop/contact/ https://cwmpas.coop/digital-society/media-literacy-in-rct/
ICO (Information Commissioner's Office)	Provides resources and information on online safety that focus on how to safely use and share information. Provides information and resources on microtargeting. Offers guidance and resources on the Children's Code, which include lesson plans and worksheets. To find out more, go to https://ico.org.uk/for-the-public/ https://ico.org.uk/for-the-public/online/social-networking/ https://ico.org.uk/for-the-public/microtargeting/ https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/

	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/school-resources/wales-secondary/
Into Film	Provides online video resources to help with teaching online safety topics. To find out more, go to https://www.intofilm.org/contact
UK Safer Internet Centre	Provides advice and resources to help children and young people stay safe online. Offers tools for educators, parents, and carers, including lesson plans, films, and policy guidance. Organises Safer Internet Day , a national event that promotes positive use of digital technology. To find out more, go to https://saferinternet.org.uk/about
Thinkuknow (by CEOP / NCA)	Run by the National Crime Agency's CEOP Command, this site offers age-specific content for children and young people, as well as resources for parents and educators. Topics include grooming, social media, image sharing, and healthy relationships online. To find out more, go to https://www.thinkuknow.co.uk
Prevent UK	Aims to influence and educate on issues such as substance abuse, crime and internet safety. Offers a range of teaching resources and lesson plans covering issues including: • internet safety • account hacking • online gaming • online dilemmas • cyberbullying • password safety To find out more, go to Resources – Prevent UK

Resources required for assessment

Assessment of this unit should not require any specific resources.

References to third-party materials and links to external websites in this document are provided for convenience and informational purposes only.

We select and review these resources at the time of publication to support teaching and learning; however, their inclusion does not imply endorsement or guarantee of the organisations, content or opinions expressed.

We do not produce, maintain or control the external materials, and therefore cannot ensure their ongoing accuracy, availability or suitability, as content may change without notice.

Any questions or concerns about external content should be directed to the original providers. If you identify any links that are no longer working or are inappropriate, you are encouraged to inform the subject team so they can be reviewed. All information in this publication is accurate at the time of publication.

© WJEC CBAC Limited 2026.