TLM Level 2 Award in eSafety - Guidance

General Information

RQF general description for Level 2 qualifications

● Achievement at RQF Level 2 (EQF Level 3) reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straight-forward problems. It includes taking responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance.

● Use an understanding of facts, procedures, and ideas to complete well-defined tasks and address straightforward problems. Interpret relevant information and ideas. Be aware of the types of information that are relevant to the area of study or work.

● Complete well-defined generally routine tasks and address straight-forward problems. Select and use relevant skills and procedures. Identify, gather and use relevant information to inform actions. Identify how effective actions have been.

● Take responsibility for completing tasks and procedures.

● Exercise autonomy and judgement subject to overall direction or guidance.

Requirements

● Standards must be confirmed by a trained Level 2 Assessor or higher.

● Assessors must at a minimum record assessment judgements as entries in the online Markbook on the INGOTs.org certification site.

● Routine evidence of work used for judging assessment outcomes in the candidates' records of their day to day work will be available from their eportfolios and online work. Assessors should ensure that relevant web pages are available to their Account Manager on request by supply of the URL.

● When the candidate provides evidence of matching all the criteria to the specification, subject to the guidance below, the assessor can request the award using the link on the certification site. The Account Manager will request a random sample of evidence from candidates' work that verifies the assessor's judgement.

● When the Account Manager is satisfied that the evidence is sufficient to safely make an award, the candidate's success will be confirmed, and the unit certificate will be printable from the web site.

● Each unit at Level 2 has recommended 40 guided learning hours based on the time required to complete by an average learner.

Assessment Method

Assessors can score each of the criteria N, L, S or H. N indicates no evidence and it is the default setting. L indicates some capability, but some help still required to meet the standard. S indicates that the candidate can match the criterion to its required specification in keeping with the overall level descriptor. H indicates performance that goes beyond the expected in at least some aspects. Candidates are required to achieve at least S on all the criteria to achieve the full unit award. Once

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

the candidate has satisfied all the criteria by demonstrating practical competence in realistic contexts, they achieve the unit certificate.

Expansion of the assessment criteria

1. Understand the Safeguarding Strategy

1.1 I can identify why an e-safety policy needs to be in place

The candidate can outline why an e-safety policy is put into place.

Evidence: From portfolios, internal testing, assessor observations.

Additional information and guidance: With the development of technology and social media, every individual who engages with social media and the internet needs to be aware of the risks to themselves and the working environment.

An e-safety policy is about ensuring all staff are aware of upholding their own reputations online, stay safe and uphold the reputation of the workplace.

1.2 I can identify guidance for safety online

The candidate will be able to describe guidance for keeping themselves safe online.

Evidence: From portfolios, internal testing, assessor observations.

Additional information and guidance: With technology changing at a vast rate, the safety guidance needs to be updated to any professionals to ensure they are aware of the current risks and how to maintain their safety. Candidates should be able to highlight the most significant risks that they face at the current time including; social media privacy settings, sharing of media online, commenting and sharing of posts and accepting friend requests etc.

1.3 I can identify the role of an Acceptable User Policy (AUP)

The candidate will be able to identify the role of the Acceptable User Policy (AUP).

Evidence: From portfolios, internal testing, assessor observations.

Additional information and guidance: The aim of an acceptable user policy (AUP) is to ensure that all staff members adhere to strict guidelines for using online services within the work environment.

The AUP will outline what is acceptable for a member of staff to undertake within the work environment. All staff members must sign an AUP document before being able to access the online services and must understand the consequences of breaking their agreement.

Each AUP created is to fit the requirements of the working environment and should have items highlighted that are suited to the online services that are used.

1.4 I can list areas that feature in the AUP

The candidate can list the different areas covered within an AUP.

Evidence: From portfolios, internal testing and/or assessor observations.

Additional information and guidance: The behaviour expected of an employee within a working environment is laid out as the code of conduct expected within the AUP. The main areas of an AUP cover the use of the internet and email within the work environment.

- No use of the internet for any illegal activities
- No attempt to break the security of the network within the working environment
- Refrain from commenting about the place of work on social media or forum sites
- Use of email is for business use only and no spam or inappropriate emails to be sent
- No downloading of programs or inappropriate content onto a work device
- Any communication using in-house methods must be professional and appropriate

All areas are fit for the company purpose and every place of work must have an individual policy that outlines their code of conduct and the sanctions that are in place should an employee break it.

2. Understand how to identify vulnerable situations

2.1 I can describe different areas of concern with technology

Candidates should be able to describe a range of concerns with the use of technology.

Evidence: From portfolios, internal testing and/or assessor observations.

Additional information and guidance: Like technology the threats that are out there increase and change regularly. Key areas all individuals should be aware of are:

Cyberbullying is bullying that takes place over any online environment or technological device.

The main issue with cyberbullying is that it does not stop as the bullying takes place on any device and there is no escape for the victim. The perpetrators feel a sense of power as they are writing it from behind a screen and cannot be identified easily. Severe cyberbullying can call for the victim to end their life and the victim feel like there is no way out. Cyberbullying is an illegal act and any concerns should click the CEOP button to report a concern.

Some news stories: https://www.bbc.co.uk/news/uk-england-berkshire-12619440 [1], https://www.youtube.com/watch?v=S03Br1dwJR8 [2]

Sexting is the sharing of inappropriate images through technology

Once you send an inappropriate image to another device, you have lost control of it. That image is no longer your possession and can and will be distributed further afield. Once an image is online it cannot be taken down and can have an instant impact on the individual’s life as well as future prospects. It is also an illegal offence to have inappropriate images on your device that are of a minor and if you send it on to others it is classed and distributing child pornography.

Trolling is the commenting on social media in a hurtful manner

Everyone has opinions of other peoples posts but when a hurtful comment is placed on a social media post it is called ‘trolling’. Unfortunately trolling can escalate very quickly when more and more people follow in the same footsteps to comment in a hurtful manner on the social media post. Trolling is the same as cyberbullying in the case that the perpetrators feel a sense of power as they are writing it from behind a screen and cannot be identified easily.

Grooming is the development of a trustful relationship over time in order to control and manipulate an individual’s actions.

With technology comes the ability to be someone else or hide your true identity. This has been the method of developing relationships with vulnerable individuals. Through the development of this trustful relationship, the groomer can manipulate the victim into circumstances and activities that they do not want to engage with.

Online radicalisation and extremism:

Radicalisation is the action or process of causing someone to adopt radical positions on political or social issues.

Extremism is the holding of extreme political or religious views; fanaticism. With the development of online environments, the threat of radicalisation and extremism has developed as there are now more options available to identify vulnerable individuals. Individuals who are seeking answers and feeling detached from society/culture/religion, seek guidance from online sources and there they can be identified and contacted.

Visit https://www.thinkuknow.co.uk/ [3] to keep up to date with current e-safety guidance

2.2 I can list who the e-safety policy applies to

The candidate should be able to list areas where the e-safety policy should be in place.

Evidence: Internal testing, assessor observations.

Additional information and guidance: All environments that utilise the internet and email services should have an e-safety policy in place. Any e-safety issue should be flagged to the designated person on site.

An AUP should be in place in all working environments that utilise email and internet services as well as an overall e-safety policy.

2.3 I can identify how to support the workplace

Candidates should be able to list how they support the workplace

Evidence: Portfolios, assessor observations.

Additional information and guidance: An individual in the workplace is expected to follow the company/workplace AUP and e-safety policy. Ensuring all sign and agree to the AUP can ensure all use of email and internet services is understood and adhered to, with a clear understanding of the

consequences for breaking any AUP sections.

All staff members should receive regular training on what e-safety threats are as well as the company/workplace AUP expectations.

Online reputation is essential not only for the individual but for the workplace. Any workplace expects its employees to uphold the company in a positive manner when posting or commenting online and should consider their actions and implications for others.

Ensuring social media accounts are secure through privacy settings and considering friend requests carefully before accepting all. In some instances, utilising an anagram of your name or using last name first can slow down people finding your social media account.

A good test to check your online presence is to add your name in quote marks in a google search. This will direct you to where personal images or details are and where your personal information is potentially being used without your permission.

3. Understand Roles and Responsibilities

3.1 I can Identify the role of an e-safety lead

Candidates should be able to list the roles and responsibilities of an e-safety lead

Evidence: Portfolios, assessor observations.

Additional information and guidance: Although not all members of staff need to fully understand the role of an e-safety lead, it is important to understand what they do and how they support you. The role of an e-safety lead needs to adapt to the situation they are in and can include; making sure all staff are aware how to raise safeguarding concerns, ensuring all staff understand the threats of using technology inappropriately.

The main areas are then broken down further to ensure that the e-safety lead manages training needs and raises awareness.

3.2 I can identify the role of all staff members

Candidates should be able to list the roles and responsibilities of a staff member

Evidence: Portfolios, assessor observations.

Additional information and guidance: Everyone who works with email or internet services is responsible for adhering to the eSafety policy and AUP set out within the workplace. If you are concerned about something you have seen in the workplace or received an inappropriate email, then it must be referred to the relevant person in the workplace.
It is every individual's role to ensure their online reputation is intact and managed to be professional not only for themselves but also for the workplace.

Moderation/verification

The assessor should keep a record of assessment judgements made for each candidate and make notes of any significant issues for any candidate. They must be prepared to enter into dialogue with their Account Manager and provide their assessment records to the Account Manager through the online Markbook. They should be prepared to provide evidence as a basis for their judgements through reference to candidate e-portfolios and any other sources e.g. through signed witness

statements associated with the criteria matching marks in the online Markbook or internal controlled testing.

Before authorizing certification, the Account Manager must be satisfied that the assessor's judgements are sound.

Source URL: https://theingots.org/community/cpdl2u1x

Links
[1] https://www.bbc.co.uk/news/uk-england-berkshire-12619440
[2] https://www.youtube.com/watch?v=S03Br1dwJR8
[3] https://www.thinkuknow.co.uk/