Open Awards Qualification Unit

This unit forms part of a regulated qualification. Click here to view qualifications.

1 Unit Details

Unit Title:	Safety and Wellbeing in a Digital Environment
Unit Reference Number:	T/618/3264
Level:	2
Credit Value:	3
Minimum GLH:	22

2 Learning Outcomes and Criteria

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Understand how to protect a range devices and data	1.1 Explain the importance of protecting a range of devices
	1.2 Explain how passwords effectively protect devices and the characteristics of strong passwords
	1.3 Explain the potential security risks associated with digital technology and social media
	1.4 Explain the importance of protecting own personal and financial data
2. Understand how to protect own devices and personal data	2.1 Explain potential types of threat to personal data and devices
	2.2 Outline the range of software and tools available to help protect data and devices
	2.3 Describe how to protect own personal information and data
	2.4 Describe how to protect financial data and transactions
3. Be able to protect own devices and personal data	3.1 Use security software effectively to protect a range of devices
	3.2 Ensure information is accessed from trustworthy sources
	3.3 Identify websites and emails which may not be

			genuine
		3.4	Discuss how to safeguard own personal and financial data
4.	Be able to protect organisational data and transactions	4.1	Discuss legislation and organisational procedures related to protection of personal and financial data
		4.2	Explain organisational procedures when finding, storing, processing and transmitting data
		4.3	Complete online transactions in line with organisational procedures using appropriate safeguards to protect individuals and the organisation
		4.4	Report inappropriate activity and potential security breaches
5.	Know how to use visual display screen equipment in line with health and safety legislation and procedures	5.1	Identify the legislation in place to protect employees
		5.2	Identify employer responsibilities to protect employees
		5.3	Demonstrate the use of display screen equipment safely and appropriately
6.	Understand how to manage own digital wellbeing	6.1	Identify the types and causes of potential physical and psychological stresses of working with devices
		6.2	Explain what action may be taken to reduce or minimise physical and psychological stress
		6.3	Identify strategies of keeping well and avoiding/overcoming cyberbullying and coercion

Learning Outcome 1 - Indicative Content

Learners must demonstrate that they understand how to protect a range of devices which they use in a personal context but also in a work-related context. Where the learner is not in work their knowledge should be tested through questioning and use of case study examples. The learner should be able to demonstrate that they understand the risks of accessing unsecured websites and downloading data from potentially unsecured sources and the importance of minimising risks to individual devices and IT systems.

In addition, they must demonstrate that they understand the risks associated with using digital technology and social media in all aspects of their personal life but also in the work environment and of the potential impact it may have on their own reputation, safety and their career. This learning outcome is relevant and important to all other units in this qualification and evidence may be cross referenced

Online safety is key to effective use of digital technology and social media and of great importance to employers as well as individual and therefore it is a critical skill that people need for their own personal and professional lives.

This outcome can be demonstrated separately or across the range of other units including managing information, content creation, communication and collaboration and digital career development

Learning Outcome 2 - Indicative Content

This outcome is about ensuring that learners understand the importance of keeping their own devices, data and financial transactions secure. They must also demonstrate an awareness of the software and tools available to keep devices and data safe and to be able to describe safe practices to ensure their data is kept secure.

Evidence will include learners describing the steps they take to protect their personal and financial data and how they apply these principles to their online activity. The principles should not only include setting and maintaining strong passwords and pins but also the risks posed by using public internet networks. They must demonstrate a good understanding of how to keep their financial transactions safe online and recognise phishing.

Damage to devices and data is always present from viruses, phishing and every changing sources. Learners should understand the impact of not protecting their devices sufficiently and develop effective routines which ensure they regularly update software to maximise the security of their devices and data.

Security of personal and financial data is critical to preventing identity fraud and learner should demonstrate that the understand the risks associated with not keeping information and data secure both for themselves and for others. The learner should also describe the risks posed by using public internet networks. These principles are key to ensuring they operate safety and securely in business environment and will appear throughout this qualification.

Learning Outcome 3 - Indicative Content

This outcome is about ensuring that learners can apply their knowledge of keeping their devices and data safe. They should demonstrate that they are able take the necessary steps to safeguard their own data, including personal and financial data and their activity on social media. This outcome will cross reference with the Digital Career Development unit.

Evidence will include learners applying the principles of online safety and security to their own online activity. The principles should not only include setting and maintaining strong passwords and pins but also the use of antivirus and anti-phishing software.

Damage to devices and data is always present from viruses, phishing and every changing sources. Learners should understand the impact of not protecting their devices sufficiently and develop effective routines which ensure they regularly update software to maximise the security of their devices and data.

Security of personal and financial data is critical to preventing identity fraud and learner should demonstrate that the understand the risks associated with not keeping information and data secure both for themselves and for others.

These principles are key to ensuring they operate safety and securely in business environment and will appear throughout this qualification.

Learning Outcome 4 - Indicative Content

This outcome requires the learner to show that they can apply their knowledge of protecting data to the work place setting and understand the legislation and organisational procedures associated with protecting organisational, personal and financial data. Learners must be able to describe the types of data that organisations collect, analyse, create, store and transmit, through questioning and/or case studies.

They must show they understand data protection laws and organisation procedures related to the protection of personal and financial data and appropriate use of technology, internet, email and social media whilst in the work place. They should also demonstrate that they understand the financial and reputational impacts of not protecting or misusing data.

Learners must also demonstrate an understanding of and follow organisational procedures when using data which should be observed or evidenced with witness testimony from the workplace supervisor

Learning Outcome 5 - Indicative Content

This outcome is about demonstrating that an individual can work in a way that protects themselves and others against health and safety risks associated with using display screen equipment and should include ergonomics. They should also demonstrate that they understand the employer's responsibility to protect employees at work and be able to discuss legislation in place to protect employees.

The learner should demonstrate they understand the common dangers of using display screen equipment, including back problems, ozone emissions, repetitive strain injury and eye strain and be able to explain how to minimise the impact of these potential problems.

Evidence for this outcome should come through observation of the learner in the workplace or classroom, through use of professional discussion and questioning and use of case studies.