| | |
|---|---|
| **Unit code** | BSBXXX113 |
| **Unit title** | Develop Intermediate Digital Safety, Wellbeing and Responsible Use Skills |
| **Unit outcomes** | This unit describes the skills and knowledge required to maintain digital safety, wellbeing and responsible use in workplace contexts.<br><br>Learners develop intermediate capability across four competence (**C**) areas:<br><br>C1. Protecting devices<br><br>C2. Protecting personal data and privacy<br><br>C3. Supporting wellbeing<br><br>C4. Environmental impacts of digital technologies.<br><br>No licensing, legislative or certification requirements apply to this unit at the time of publication. |
| **Knowledge (K)** | Required knowledge includes:<br>K1. Analyse the main features of how Artificial Intelligence (AI) systems can be used for both cyber attacks and cyber security.<br><br>K2. Recognise key concepts of data protection and privacy legislation and understand the complexity of personal data ownership in AI systems.<br><br>K3. Describe privacy implications associated with online content sharing, including its use in AI training.<br><br>K4. Explain the main features and functions of privacy tools.<br><br>K5. Evaluate reliable information sources and inclusive groups or communities that support physical, mental and social wellbeing.<br><br>K6. Analyse examples of harmful content and behaviour and their impacts.<br><br>K7. Describe how digital technologies, including social media, can amplify bias, stereotyping and exclusion.<br><br>K8. Outline strategies to protect against, or respond to, harmful behaviour or content when they are encountered.<br><br>K9. Analyse environmental impacts of digital technologies across manufacturing, usage and disposal, including impacts of data centres and e-commerce.<br><br>K10. Describe how digital tools can support sustainable living.<br><br>K11. Define concepts of collaborative consumption and strategies to extend device lifecycles, including associated risks, limitations and environmental benefits. |
| **Skills (S)** | Required skills include:<br>S1. Apply a range of prevention techniques to protect devices and their contents. |

| | |
|---|---|
| | S2. Manage personal data and privacy across varied digital environments, including effective use of privacy tools.<br>S3. Analyse and adapt personal digital usage patterns to support physical, mental and social wellbeing.<br>S4. Implement strategies to protect against, and respond effectively to, harmful behaviour and content.<br>S5. Apply strategies to reduce environmental impacts of digital technology use, including device purchasing, usage, repair, recycling and disposal. |
| **Application of Knowledge & Skills** | At the Intermediate level, learners apply knowledge (K1-K11) and skills (S1-S5) with some autonomy across all competence areas (C1-C4) with the following characteristics:<br>• Autonomy: With some autonomy under limited supervision, making informed decisions about safety and protection approaches within established workplace frameworks and procedures.<br>• Accountability: Accountable for quality and effectiveness of their own digital safety practices and for supporting others with routine safety and wellbeing tasks.<br>• Responsibility: Responsible for selecting appropriate protection strategies and privacy tools to achieve workplace outcomes within defined parameters.<br>• Context: Varied workplace safety and wellbeing tasks of moderate complexity, adapting approaches to different contexts while working within organisational guidelines.<br>• Decision-Making: Make informed decisions about security threat prevention, privacy management and wellbeing strategies; seek guidance when facing unfamiliar situations, ethical considerations, or requirements beyond established procedures. |
| **Assessment Requirements** | |
| **Performance evidence (PE)** | Learners must demonstrate ability to:<br>PE1. apply prevention techniques to protect devices and their contents in accordance with workplace procedures, including recognising AI systems used in cyber attacks and cyber security<br>PE2. manage personal data and privacy across varied digital environments using workplace criteria, including use of privacy tools<br>PE3. analyse and adapt digital usage patterns to support physical, mental and social wellbeing<br>PE4. implement strategies to respond to harmful behaviour and content<br>PE5. apply environmental sustainability strategies throughout the device lifecycle, including informed purchasing, usage, repair and disposal decisions. |

| | |
|---|---|
| | Performance evidence must be demonstrated across at least two different workplace scenarios. |
| **Knowledge evidence (KE)** | Learners must demonstrate knowledge of:<br>KE1. role of AI systems in both cyber attacks and cyber security<br>KE2. data protection and privacy legislation concepts, including anonymisation, pseudonymisation, data removal rights, and personal data breaches<br>KE3. AI-related privacy implications, including data ownership complexity and use of shared content for AI training<br>KE4. privacy tools and their features and functions<br>KE5. sources of information and communities supporting physical, mental and social wellbeing in digital environments<br>KE6. harmful digital content and behaviour, associated impacts, and how digital technologies can amplify bias, stereotyping and exclusion<br>KE7. strategies to protect against, or respond to, harmful behaviour<br>KE8. environmental impacts of digital technologies across device lifecycles, data centres and e-commerce, including collaborative consumption and lifecycle extension concepts.<br>Knowledge evidence must be demonstrated across at least two different workplace scenarios. |
| **Assessment conditions** | Assessment must be conducted in workplace or simulated environments that reflect real workplace conditions, including access to:<br>• digital devices and platforms requiring security threat prevention and privacy management<br>• scenarios involving personal data protection decisions across varied contexts<br>• opportunities to analyse digital usage patterns and apply wellbeing strategies<br>• contexts requiring environmentally sustainable decisions across device lifecycles<br>• organisational procedures for security, privacy, wellbeing and environmental sustainability<br>• assistive technologies as required to support diverse learner needs.<br>Assessors must satisfy the requirements for assessors under applicable VET legislation, frameworks, and standards. |
| **Unit Mapping Information** | No equivalent unit. |
| **Links** | Link to BSB TP Companion Volume Implementation Guide. |