Unit code	BSBXXX137
Unit title	Develop Digital Safety, Wellbeing and Responsible Use Skills
Unit outcomes	This unit describes a progressive pathway for developing workplace cyber security capability across four proficiency levels: Basic, Intermediate, Advanced and Highly Advanced. Learners may enter at a proficiency level aligned to existing capability and may exit upon successful completion of their target proficiency level without completing the entire progression. Recognition of Prior Learning and assessment-only pathways are supported. Learners develop capability across four competence (C) areas: C1. Protecting devices C2. Protecting personal data and privacy C3. Protecting health and wellbeing C4. Protecting the environment. No licensing, legislative or certification requirements apply to this unit at the time of publication.
Knowledge (K)	Basic level Required knowledge includes: K1. Concepts of cyber security, cyber threats and cyber attacks, and how individual actions and cyber security tools work together. K2. Basic device protection measures such as antivirus software, screen locking, strong passwords and multi-factor authentication. K3. How personal data is collected and generated, and that privacy rights are protected under legislation. K4. Risks associated with sharing personal data, including Artificial Intelligence (AI)-related risks. K5. Signs of identity theft and options for blocking or flagging inappropriately shared information. K6. Key risks and benefits to wellbeing in digital environments. K7. Platform features designed to capture attention, and the limitations of virtual assistants and AI systems in supporting human wellbeing. K8. Strategies and supports for wellbeing in digital environments, and signs of problematic digital usage. K9. Environmental impacts of digital technologies, including AI systems and data centres. K10. Simple strategies to reduce energy use and data consumption. Intermediate level Required knowledge includes: K11. Features of the use of AI systems in cyber attacks and cyber security. K12. Key concepts in data protection and privacy legislation including anonymisation, pseudonymisation, data removal rights and data breaches.

	K13. Privacy implications of online content use, including AI training, and privacy tools and their functions. K14. Reliable information sources and inclusive communities that support wellbeing. K15. Harmful content and behaviours and how digital technologies can reinforce bias, stereotyping and exclusion. K16. Environmental impacts across manufacturing, usage and disposal of digital technologies. K17. Sustainable digital practices, including collaborative consumption and device lifecycle extension. Advanced level Required knowledge includes: K18. Individual rights under cyber security legislation and how emerging technologies, including AI systems, are used in cyber threats and protection. K19. Data protection and privacy rights to support others to understand and apply protection strategies. K20. Wellbeing and inclusion rights relevant to digital environments. K21. Harmful behaviour, content and deceptive design practices that contribute to bias and exclusion. K22. Environmental impacts of digital technologies to support evaluation, decision-making and guidance of others. Highly Advanced level Required knowledge includes: K23. Emerging developments and trends in cyber security technologies and legislation. K24. Frameworks and methodologies for designing cyber security initiatives, data protection and privacy strategies, wellbeing and inclusion programs, and digital sustainability solutions. K25. Ethical practices and proportionate use of technologies in digital safety, wellbeing and sustainability contexts. K26. Approaches to building digital safety, privacy, wellbeing and environmental responsibility capability in others.
Skills (S)	Basic level Required skills include: S1. Apply basic device and personal data protection measures and respond to identity theft indicators. S2. Assess and adjust personal digital habits to support wellbeing. S3. Apply simple strategies to reduce the environmental impact of digital technologies. Intermediate level Required skills include: S4. Apply a variety of malware prevention techniques. S5. Manage personal data and privacy using appropriate tools.

	S6. Analyse and adapt personal digital usage to support wellbeing. S7. Implement strategies to protect oneself against harmful behaviour and content. S8. Apply environmentally responsible practices across device lifecycles. Advanced level Required skills include: S9. Update cyber security measures to address emerging threats. S10. Support others to understand data protection and privacy rights and implement strategies to protect personal data and manage privacy. S11. Assist others to adapt digital use to support wellbeing, and understand their rights in relation to inclusion and wellbeing in digital environments. S12. Flag or intervene in instances of harmful behaviour or content in digital environments. S13. Assist others to develop awareness of harmful behaviour, content and deceptive design, and build capacity to counter bias, stereotyping and exclusion. S14. Evaluate environmental impacts of digital technologies and support others to reduce their impact. Highly Advanced level Required skills include: S15. Inform strategic decision-making through awareness of developments in cyber security and privacy technologies and legislation. S16. Lead or contribute to organisational cyber security initiatives. S17. Support others to build their capabilities in protecting devices and contents against digital threats. S18. Advise on policy or regulatory aspects of data protection and privacy in digital contexts. S19. Design personal data and privacy protection strategies. S20. Lead or contribute to wellbeing and inclusion initiatives. S21. Lead or contribute to digital sustainability initiatives.
Application of Knowledge & Skills	Basic level Learners apply knowledge and skills under direct guidance and supervision, following clear instructions in straightforward routine tasks within familiar workplace contexts; accountable for completing assigned tasks accurately; escalate when encountering unfamiliar situations. Intermediate level Learners apply knowledge and skills with some autonomy under limited supervision, making informed decisions in varied tasks of moderate complexity; accountable for quality of their own work and supporting others with routine tasks; seek guidance when facing unfamiliar situations or ethical considerations. Advanced level

	Learners apply knowledge and skills with significant autonomy and initiative, making strategic decisions in tasks requiring analysis across diverse contexts; accountable for outcomes of their own and others' work; responsible for guiding others and contributing to capability development; identify when specialist expertise is required. Highly Advanced level Learners apply knowledge and skills independently with full accountability, exercising leadership in strategy development and organisational transformation; accountable for organisational capability and strategic outcomes; responsible for leading initiatives, establishing governance frameworks, and driving cultural change; determine when external expertise or board-level approval is required.
Assessment Requirements	
Performance evidence (PE)	Assessment must be conducted at the learner's target proficiency level, with assessors recognising that higher-level performance inherently incorporates lower-level competencies. Basic level Learners must demonstrate ability to: PE1. Apply device protection measures in accordance with workplace procedures. PE2. Implement basic personal data protection measures. PE3. Assess personal digital habits and apply personalised strategies to support wellbeing. PE4. Apply environmentally responsible practices when using digital technologies. Intermediate level Learners must demonstrate ability to: PE5. Apply malware prevention techniques to protect devices and digital content following workplace procedures. PE6. Manage personal data and privacy across varied digital environments using workplace criteria, privacy tools and awareness of AI-related privacy implications. PE7. Analyse and adapt digital usage patterns to support wellbeing, and implement strategies to protect against and respond to harmful behaviour and content. PE8. Apply environmentally sustainable practices across the device lifecycle. Advanced level Learners must demonstrate ability to:

	PE9. Update cyber security measures in response to evolving threats and support others to implement effective device protection measures. PE10. Support others to understand data protection and privacy rights and assist in applying strategies to manage personal data and privacy in digital environments. PE11. Assist others to review and adapt their digital usage to support wellbeing, intervene or flag harmful behaviour, counter bias and exclusion, and promote inclusive digital practices. PE12. Evaluate environmental impacts of digital technologies to inform decision-making or advocacy and assist others to assess and reduce their environmental impact. Highly Advanced level Learners must demonstrate ability to: PE13. Lead or contribute to organisational cyber security initiatives. PE14. Build organisational capability in device protection. PE15. Advise on data protection and privacy policy, and lead or contribute to the design of personal data protection strategies in digital contexts. PE16. Lead or contribute to wellbeing and inclusion initiatives in digital environments. PE17. Understand and apply relevant legislative and regulatory requirements in organisational contexts. PE18. Promote environmentally sustainable digital practices, and lead or contribute to digital sustainability initiatives. Performance evidence must be demonstrated across at least two different workplace scenarios.
Knowledge evidence (KE)	Basic level Learners must demonstrate knowledge of: KE1. Core cyber security concepts, common digital threats, and basic device protection measures. KE2. How individual actions and cyber security tools work together to protect devices. KE3. How personal data is collected and generated, privacy rights, and risks associated with data sharing including AI-related risks. KE4. Signs of identity theft, manipulative or deceptive digital practices, and options for blocking or flagging inappropriately shared information. KE5. Risks and benefits to wellbeing in digital environments, including attention-capturing platform features and limitations of AI systems for wellbeing support.

	KE6. Environmental impacts of digital technologies including AI systems and data centres, and basic strategies to reduce energy and data consumption. Intermediate level Learners must demonstrate knowledge of: KE7. Features of malware and the use of AI systems in both cyber attacks and cyber security. KE8. Key concepts in data protection and privacy legislation, including privacy, anonymisation, pseudonymisation, data removal rights, and personal data breaches. KE9. AI-related privacy implications, including data ownership complexity and use of shared content for AI training. KE10. Data protection and privacy tools, their features and functions. KE11. Reliable sources of information and inclusive communities that support wellbeing in digital environments. KE12. Harmful digital content and behaviours, their impacts, and how digital technologies can amplify bias, stereotyping and exclusion. KE13. Strategies to protect against, respond to and report harmful behaviour or content. KE14. Environmental impacts across device lifecycles, data centres and e-commerce, including concepts of collaborative consumption and device lifecycle extension. Advanced level Learners must demonstrate knowledge of: KE15. Key rights of individuals under current cyber security legislation. KE16. Examples of how emerging technologies, including AI systems, are used in cyber threats and cyber security responses. KE17. Data protection and privacy rights to support others to understand and apply protection strategies. KE18. Wellbeing and inclusion rights relevant to digital environments. KE19. Harmful behaviour, content and deceptive design practices that contribute to bias and exclusion. KE20. Environmental impacts of digital technologies to support evaluation, decision-making and guidance of others. Highly Advanced level Learners must demonstrate knowledge of: KE21. Emerging developments and trends in cyber security technologies and legislation. KE22. Legislation, frameworks and methodologies to inform design of cyber security initiatives, data protection and privacy strategies,

	wellbeing and inclusion programs, and digital sustainability solutions. KE23. Ethical practices and proportionate use of technologies in digital safety, wellbeing and sustainability contexts. KE24. Approaches to building digital safety, privacy, wellbeing and environmental responsibility capability in others. Knowledge evidence must be demonstrated across at least two different workplace scenarios.
Assessment conditions	Assessment must occur in conditions that reflect typical or simulated workplace environments appropriate to the target proficiency level, with higher-level assessment inherently incorporating lower-level requirements. All levels require access to: • digital devices and platforms requiring security measures and protection practices • opportunities to implement and monitor protection measures • organisational procedures for security, privacy, wellbeing and environmental sustainability • assistive technologies where required to support diverse learner needs. Additionally, by proficiency level: Basic: • digital security tools and platforms used in workplace contexts • scenarios involving personal data handling, online transactions, and privacy management • opportunities to assess digital habits and implement wellbeing strategies • contexts allowing application of environmentally responsible digital practices • established workplace procedures providing clear guidance. Intermediate: • various digital devices, platforms, and security features • scenarios involving personal data protection decisions across varied contexts • opportunities to analyse digital usage patterns and implement wellbeing strategies • contexts requiring environmental sustainability decisions throughout device lifecycles

	• organisational procedures for malware prevention and privacy management. Advanced: • digital devices and platforms requiring cyber security updates and protection guidance • scenarios requiring support of others in understanding rights and implementing protection strategies • opportunities to assist others in wellbeing adaptation and intervention in harmful situations • contexts requiring environmental impact evaluation and guidance of others • situations requiring management of challenging interactions and promotion of inclusive behaviour. Highly Advanced: • comprehensive digital safety platforms requiring strategic governance • scenarios involving specialised challenges requiring integrated responses • opportunities to design, implement and evaluate transformation initiatives • contexts requiring leadership and capability building of others in advanced digital safety practices • emerging technologies and platforms requiring strategic assessment and integration • legislative and policy frameworks requiring interpretation and application. 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.