

Unit code	BSBXXX105
Unit title	Develop Basic Digital Safety, Wellbeing and Responsible Use Skills
Unit outcomes	<p>This unit describes the skills and knowledge required to maintain digital safety, wellbeing and responsible use in workplace contexts.</p> <p>Learners develop capability across four competence (C) areas:</p> <p>C1. Protecting devices</p> <p>C2. Protecting personal data and privacy</p> <p>C3. Supporting wellbeing</p> <p>C4. Environmental impacts of digital technologies</p> <p>No licensing, legislative or certification requirements apply to this unit at the time of publication.</p>
Knowledge (K)	<p>Required knowledge includes:</p> <p>K1. Recognise cyber security concepts, and that individual actions and cyber security tools work together to protect devices.</p> <p>K2. Identify basic digital device protection measures.</p> <p>K3. Recognise that cyber security legislation helps ensure security of products and services.</p> <p>K4. Recognise that personal data is collected and generated through digital sources and processes, and privacy rights are protected under legislation.</p> <p>K5. Identify risks associated with sharing personal data in digital environments.</p> <p>K6. Recognise signs of identity theft.</p> <p>K7. Identify main risks and benefits to physical, mental and social wellbeing in digital environments.</p> <p>K8. Identify digital platform features designed to capture and maintain attention and recognise limitations and risks of using virtual assistants and Artificial Intelligence (AI) systems to support human wellbeing.</p> <p>K9. Identify strategies to support physical, mental and social wellbeing in digital environments, recognise signs and potential effects of problematic digital usage, and that laws and regulations help protect wellbeing.</p> <p>K10. Recognise that some digital technologies and infrastructures have significant environmental impacts.</p> <p>K11. Recognise that digital technologies can support energy efficiency and sustainability.</p>
Skills (S)	<p>Required skills include:</p> <p>S1. Follow workplace procedures to use basic device protection measures.</p>

	<p>S2. Follow basic security measures for online payments and transactions.</p> <p>S3. Follow workplace procedures to respond to signs of identity theft.</p> <p>S4. Follow workplace procedures to block or flag personal information that has been shared inappropriately.</p> <p>S5. Use workplace wellbeing guidelines to support personal digital habits.</p> <p>S6. Follow simple strategies to reduce energy and data consumption of digital technologies.</p>
Application of Knowledge and Skills	<p>At the Basic level, learners apply knowledge (K1-K11) and skills (S1-S6) across all competence areas (C1-C4) with the following characteristics:</p> <ul style="list-style-type: none"> • Autonomy: Under direct guidance and supervision, following clear instructions and established workplace procedures. • Accountability: Accountable for completing assigned digital safety tasks accurately and following workplace security, privacy and wellbeing requirements. • Context: Straightforward, routine workplace digital safety tasks using workplace-approved security measures and established wellbeing guidelines within familiar workplace contexts. • Decision-Making: Make routine decisions about security measures and wellbeing practices within established guidelines; escalate to supervisor when encountering security threats, privacy breaches, or wellbeing concerns requiring guidance.
Assessment Requirements	
Performance evidence (PE)	<p>Learners must demonstrate ability to:</p> <p>PE1. follow workplace procedures to use device protection measures</p> <p>PE2. follow workplace procedures for personal data security</p> <p>PE3. use workplace wellbeing guidelines to review digital habits and support personal wellbeing</p> <p>PE4. follow environmentally responsible practices when using digital technologies.</p> <p>Performance evidence must be demonstrated across at least two different workplace scenarios.</p>
Knowledge evidence	<p>Learners must demonstrate knowledge of:</p> <p>KE1. cyber security concepts and device protection measures</p> <p>KE2. personal data collection, privacy rights, and data sharing risks</p> <p>KE3. identity theft indicators, manipulative methods, and procedures for blocking or flagging personal information</p> <p>KE4. risks and benefits to physical, mental and social wellbeing in digital environments</p>

	<p>KE5. environmental impacts of digital technologies and strategies to support sustainability.</p> <p>Knowledge evidence must be demonstrated across at least two different workplace scenarios.</p>
Assessment conditions	<p>Assessment must be conducted in a workplace or simulated environment that accurately reflects real workplace conditions, and includes access to:</p> <ul style="list-style-type: none"> • digital devices and platforms requiring security measures • scenarios involving personal data handling, online transactions, and privacy management • opportunities to use wellbeing guidelines related to digital use • contexts allowing application of environmentally responsible digital practices • organisational procedures for security, privacy, wellbeing and environmental sustainability • assistive technologies as required. <p>Assessors must satisfy the requirements for assessors under applicable VET legislation, frameworks, and standards.</p>
Unit Mapping Information	No equivalent unit.
Links	Link to BSB TP Companion Volume Implementation Guide.