

Unit code	BSBXXX129
Unit title	Develop Highly Advanced Digital Safety, Wellbeing and Responsible Use Skills
Unit outcomes	<p>This unit describes the skills and knowledge required to drive digital safety, wellbeing and responsible use initiatives and drive organisational transformation.</p> <p>Learners develop highly advanced 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. emerging developments in cyber security technologies, data protection and privacy solutions, and environmental sustainability impacts</p> <p>K2. legislative and regulatory frameworks for cyber security, data protection, wellbeing and sustainability</p> <p>K3. methods for designing cyber security initiatives, data protection strategies and wellbeing programs</p> <p>K4. ethical and responsible use of digital technologies, including governance principles and risk management</p> <p>K5. approaches for building capability in others across digital safety, wellbeing and sustainability.</p>
Skills (S)	<p>Required skills include:</p> <p>S1. Stay informed about developments in cyber security technologies and legislation.</p> <p>S2. Interpret and assess rights and obligations under cyber security legislation.</p> <p>S3. Lead citizen-focused cyber security initiatives.</p> <p>S4. Build capability in others in device and content protection practices.</p> <p>S5. Stay informed about developments in data ownership, privacy technologies and regulatory frameworks.</p> <p>S6. Provide advice on policy and regulatory requirements for data protection.</p>

	<p>S7. Lead design and implementation of organisation-wide data protection strategies.</p> <p>S8. Champion inclusive and wellbeing-focused practices in digital environments.</p> <p>S9. Evaluate wellbeing and inclusion evidence to guide decision-making.</p> <p>S10. Lead initiatives that embed wellbeing and inclusion into digital systems and practices.</p> <p>S11. Contribute to legal and regulatory decision-making relating to digital wellbeing and inclusion.</p> <p>S12. Stay informed about environmental and sustainability impacts of digital technologies.</p> <p>S13. Promote sustainable and responsible use of digital technologies.</p> <p>S14. Lead digital sustainability initiatives and transformation programs.</p> <p>S15. Contribute to development of innovative solutions that improve digital sustainability.</p>
<p>Application of Knowledge & Skills</p>	<p>At the Highly Advanced level, learners apply knowledge (K1-K5) and skills (S1-S15) with full autonomy across all competence areas (C1-C4) with the following characteristics:</p> <ul style="list-style-type: none"> • Autonomy: Independently and with full accountability, exercising leadership in safety, wellbeing and sustainability strategy development, policy formulation, and organisational transformation initiatives. • Accountability: Accountable for organisational digital safety, wellbeing and sustainability capability, strategic outcomes, governance frameworks, and the development of organisational systems and practices. • Responsibility: Responsible for leading organisational safety, wellbeing and sustainability initiatives, establishing governance frameworks, building organisational capability, and driving cultural change. • Context: Highly complex, strategic organisational safety, wellbeing and sustainability challenges requiring systems thinking, governance expertise, and ability to integrate digital safety considerations with organisational strategy, risk management, and compliance frameworks across enterprise contexts. • Decision-Making: Make authoritative decisions on cyber security approaches and data protection strategies; establish organisational policies and governance frameworks for wellbeing, inclusion and environmental sustainability; lead strategic reviews and capability assessments; determine when external expertise, regulatory consultation, or board-level approval is required.

Assessment Requirements	
Performance evidence (PE)	<p>Learners must demonstrate ability to:</p> <p>PE1. assess and interpret cyber security legislation and lead citizen-focused cyber security initiatives</p> <p>PE2. provide advice on data protection and privacy policy requirements</p> <p>PE3. design and implement organisation-wide data protection strategies</p> <p>PE4. lead responsible and ethical digital governance, including oversight of risk and accountability</p> <p>PE5. evaluate wellbeing and inclusion evidence and lead initiatives that embed wellbeing into digital systems</p> <p>PE6. contribute to digital transformation decision-making</p> <p>PE7. promote sustainable use of digital technologies and lead sustainability initiatives</p> <p>PE8. mentor others to build device and content protection capability.</p> <p>Performance evidence must be demonstrated across at least two different workplace scenarios.</p>
Knowledge evidence (KE)	<p>Learners must demonstrate knowledge of:</p> <p>KE1. emerging developments in cyber security technologies, data protection and privacy solutions, and environmental sustainability impacts</p> <p>KE2. legislative and regulatory frameworks for cyber security, data protection, wellbeing and sustainability</p> <p>KE3. methods for designing cyber security initiatives, data protection strategies and wellbeing programs</p> <p>KE4. ethical and responsible use of digital technologies, including governance principles and risk management</p> <p>KE5. approaches for building capability in others across digital safety, wellbeing and sustainability.</p> <p>Knowledge evidence must be demonstrated across at least two different workplace scenarios.</p>
Assessment conditions	<p>Assessment must occur in workplace or simulated conditions that reflect real-world environments, including access to:</p> <ul style="list-style-type: none"> • advanced digital safety and sustainability platforms requiring strategic integration • scenarios involving highly complex protection, wellbeing or sustainability challenges • opportunities to design, implement and evaluate transformation initiatives

	<ul style="list-style-type: none"> • contexts requiring leadership and capability development of others • emerging technologies requiring critical assessment • legislative and policy frameworks requiring interpretation and application • assistive technologies where required to support diverse learner needs. <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.

DRAFT