BSB Companion Volume Implementation Guide

Digital Capability Appendix

DRAFT

Future Skills Organisation is a Jobs and Skills Council funded by the Australian Government Department of Employment and Workplace Relations. PO Box 16194, Collins Street West, Melbourne VIC 8007.

Version number	Stage	Date
1.0	Public and Government Consultation	01/03/2026
2.0	Technical Committee Feedback	10/06/2026

Table of Contents

About This Guide **4**
Design Approach **4**
Capability Areas **4**
Proficiency Levels **4**
Part A: Design Overview **5**
Section 1 – Purpose and Alignment **5**
1.1 Purpose 5
1.2 Framework Alignment 5
DigComp 3.0 – European Digital Competence Framework (2025) 5
Foundation Skills: Australian Core Skills Framework (ACSF) (2012) 5
Integrated Design 5
Section 2 – Digital Capability Areas **6**
Section 3 – Assessment Design and Contextualisation **7**
3.1 Assessment Approach 7
3.2 Simulated Assessment 7
3.3 Foundation Skills in Assessment 8
3.4 Contextualisation 9
Sector contextualisation examples 9
3.5 Example of Delivery Models 10
3.6 Trainer and Assessor Capability 10
3.7 Delivery of UoCs 10
3.8 ASK Template 11
Practical guidance for RTOs 11
Part B: Implementation Guidance and Reference Materials **12**
Section 1 – Digital Capability Area Reference **12**
Basic Level Units — BSBDIG201X–208X 12
BSBDIG201X — Develop Basic Digital Information Search, Evaluation and Management Skills 12
BSBDIG202X — Develop Basic Digital Communication and Collaboration Skills 13
BSBDIG203X — Develop Basic Digital Content Creation Skills 15
BSBDIG204X — Develop Basic Digital Safety, Wellbeing and Responsible Use Skills 16
BSBDIG205X — Develop Basic Digital Problem Identification and Solving Skills 17
BSBDIG206X — Develop Basic Digital Artificial Intelligence (AI) Skills 19
BSBDIG207X — Develop Basic Digital Cyber Security Skills 20
BSBDIG208X — Develop Basic Digital Skills in the Workplace 22
Intermediate Level Units — BSBDIG301X–308X 24
BSBDIG301X — Develop Intermediate Digital Information Search, Evaluation and Management Skills 24
BSBDIG302X — Develop Intermediate Digital Communication and Collaboration Skills 25
BSBDIG303X — Develop Intermediate Digital Content Creation Skills 27
BSBDIG304X — Develop Intermediate Digital Safety, Wellbeing and Responsible Use Skills 29
BSBDIG305X — Develop Intermediate Digital Problem Identification and Solving Skills 30
BSBDIG306X — Develop Intermediate Digital Artificial Intelligence (AI) Skills 31
BSBDIG307X — Develop Intermediate Digital Cyber Security Skills 33
BSBDIG308X — Develop Intermediate Digital Skills in the Workplace 34
Advanced Level Units — BSBDIG401X–408X 37
BSBDIG401X — Develop Advanced Digital Information Search, Evaluation and Management Skills 37
BSBDIG402X — Develop Advanced Digital Communication and Collaboration Skills 38
BSBDIG403X — Develop Advanced Digital Content Creation Skills 40
BSBDIG404X — Develop Advanced Digital Safety, Wellbeing and Responsible Use Skills 42
BSBDIG405X — Develop Advanced Digital Problem Identification and Solving Skills 43

DRAFT

BSBDIG406X — Develop Advanced Digital Artificial Intelligence (AI) Skills....45
BSBDIG407X — Develop Advanced Digital Cyber Security Skills....46
BSBDIG408X — Develop Advanced Digital Skills in the Workplace....48
Highly Advanced Level Units — BSBDIG501X–508X....50
BSBDIG501X — Develop Highly Advanced Digital Information Search, Evaluation and Management Skills50
BSBDIG502X — Develop Highly Advanced Digital Communication and Collaboration Skills....52
BSBDIG503X — Develop Highly Advanced Digital Content Creation Skills....54
BSBDIG504X — Develop Highly Advanced Digital Safety, Wellbeing and Responsible Use Skills....55
BSBDIG505X — Develop Highly Advanced Digital Problem Identification and Solving Skills....57
BSBDIG506X — Develop Highly Advanced Digital Artificial Intelligence (AI) Skills....58
BSBDIG507X — Develop Highly Advanced Digital Cyber Security Skills....60
BSBDIG508X — Develop Highly Advanced Digital Skills in the Workplace....62
Section 2 – Recognition of Prior Learning Guidance....66
2.1 Overview....66
2.2 Quick-reference digital capability matrix....66
2.2 RPL Guidance by Digital Capability Area....68
2.2.1 Information Search, Evaluation and Management....68
2.2.2 Communication and Collaboration....71
2.2.3 Digital Content Creation....74
2.2.4 Digital Safety, Wellbeing and Responsible Use....77
2.2.5 Digital Problem Identification and Solving....80
2.2.6 AI....83
2.2.7 Cyber Security....86
2.2.8 Digital Skills in the Workplace....89
2.3 Priority Cohort Guidance....93
Section 3 – Resource Listing....95
3.1 Key Frameworks and References....95
3.2 VET Regulations and Standards....95
3.3 Indigenous Data Sovereignty Resources....96
3.4 Implementation Resources....96

DRAFT

About This Guide

This Companion Volume Implementation Guide (CVIG) Appendix provides guidance for Registered Training Organisations (RTOs) implementing the Digital Capability Units of Competency (UoCs) within the Business Services (BSB) Training Package.

The 32 Digital Capability UoCs develop generalist digital workplace capabilities aligned to internationally and nationally recognised frameworks. They support nationally consistent training, assessment and recognition of prior learning across all industries and qualification contexts.

These units develop transferable digital capability for workers across all sectors. Examples include: healthcare, construction, retail, hospitality, manufacturing, education, professional services, community services and more. The UoCs are not sector-specific; they are designed for contextualisation into any industry setting.

Design Approach

The 32 UoCs are organised across two design approaches:

- 28 individual UoCs – targeting focused capability development within a single competence area, across four proficiency levels
- 4 horizontal UoCs – integrating the five DigComp 3.0 digital capability areas at a single proficiency level, supporting broad digital workplace capability.

Capability Areas

Seven digital capability areas are covered across the suite: five drawn directly from DigComp 3.0, and two contemporary additions reflecting Australian workforce priorities.

DigComp 3.0 digital capability areas:

- Information Search, Evaluation and Management
- Communication and Collaboration
- Digital Content Creation
- Digital Safety, Wellbeing and Responsible Use
- Digital Problem Identification and Solving

Contemporary areas:

- AI
- Cyber Security

Proficiency Levels

DigComp 3.0 defines proficiency levels as the combination of cognitive demand, task complexity and level of autonomy an individual can manage when applying a digital competence. The UoCs adopt DigComp 3.0's four proficiency levels: Basic, Intermediate, Advanced and Highly Advanced, applying this same progression consistently across all seven digital capability areas.

Level	Capability Focus
Basic	Routine digital workplace tasks, completed with guidance as needed
Intermediate	Well-defined digital workplace tasks and problems, addressed autonomously
Advanced	Specialised digital workplace tasks with autonomy, guiding others as required
Highly Advanced	Specialised digital workplace tasks with autonomy and accountability, creating new solutions and leading others

DRAFT

Part A: Design Overview

Section 1 – Purpose and Alignment

1.1 Purpose

The Digital Capability UoCs address a clearly identified national need for a suite of nationally recognised, industry-agnostic units that develop the digital capability of the Australian workforce across all industries, occupations and qualification levels.

The UoCs respond to increasing employer demand for workers who can confidently, safely and ethically use digital technologies, adapt to changing digital environments, and apply digital capability to improve workplace performance, collaboration and innovation.

The UoCs are not Information and Communications Technology (ICT) specialist units. Rather, they develop transferable workplace digital capability that can be applied in any industry or occupation. They provide a progression from Basic through to Highly Advanced, reflecting increasing autonomy, judgement, responsibility, accountability and complexity of workplace application.

The UoCs have been designed using a capability-based approach, integrating Knowledge, Skills, Performance Evidence and Knowledge Evidence to reflect authentic workplace capability.

1.2 Framework Alignment

The Digital Capability UoCs draw on internationally and nationally recognised frameworks that together provide a coherent capability architecture.

DigComp 3.0 – European Digital Competence Framework (2025)

DigComp 3.0 provides the overarching design architecture for the Digital Capability suite. It was selected because it is a leading digital competence framework for citizens, education and work, providing a comprehensive, internationally recognised structure that is applicable across industries and occupations.

DigComp 3.0 contributes:

- the five digital capability areas
- the four proficiency levels
- the progression model underpinning learner capability development.

The Digital Capability UoCs adopt these digital capability areas, with AI and Cyber Security added as Australian additions that sit alongside, rather than modify, the DigComp 3.0 framework.

Foundation Skills: Australian Core Skills Framework (ACSF) (2012)

Foundation Skills are explicitly addressed throughout every UoC in accordance with the Training Package Organising Framework (TPOF). The ACSF provides the reference framework for Learning, Reading, Writing, Oral Communication and Numeracy, operating at ACSF Level 1–2 (Basic), 2–3 (Intermediate), 3–4 (Advanced) and 4–5 (Highly Advanced).

Integrated Design

Together these frameworks form a single integrated capability architecture rather than a collection of independent references.

DigComp 3.0 provides the overall structure through its five digital capability areas and four proficiency levels. The AI and Cyber Security frameworks align with this structure by incorporating contemporary workplace capabilities

DRAFT

while maintaining alignment with the DigComp 3.0 progression model. The ACSF provides the foundation skills and digital competence architecture that is embedded consistently throughout every UoC.

As a result, learners progress through one coherent digital capability model with increasing levels of autonomy, leadership and organisational responsibility, rather than progressing through multiple independently aligned components.

Section 2 – Digital Capability Areas

The seven digital capability areas provide the organising structure for the 32 units. The first five are drawn from DigComp 3.0; AI and Cyber Security are Australian additions that sit alongside, rather than modify, the DigComp 3.0 framework.

Each area is set out below, showing its DigComp 3.0 competencies (where applicable), focus and scope.

1. Information Search, Evaluation and Management	
DigComp 3.0 competencies	1.1 Browsing, searching and filtering information 1.2 Evaluating information 1.3 Managing information
Focus	Locating, evaluating, organising and managing digital information and data.
Includes	Information searching and filtering; source evaluation and credibility assessment; managing misinformation and disinformation; file and data management; data governance and ethical information handling.

2. Communication and Collaboration	
DigComp 3.0 competencies	2.1 Interacting through and with digital technologies 2.2 Sharing through digital technologies 2.3 Engaging in citizenship through digital technologies 2.4 Collaborating through digital technologies 2.5 Digital behaviour 2.6 Managing digital identity
Focus	Using digital tools to communicate, collaborate and participate in workplace and online environments.
Includes	Digital interaction and sharing; collaboration in digital environments; digital citizenship; digital behaviour and netiquette; digital identity management.

3. Digital Content Creation	
DigComp 3.0 competencies	3.1 Developing digital content 3.2 Integrating and re-elaborating digital content 3.3 Copyright and licences 3.4 Computational thinking and programming
Focus	Creating, editing and adapting digital content across formats and tools.
Includes	Content development, integration and adaptation; copyright and licences; computational thinking and programming; accessibility in content design; ethical and transparent AI use in content workflows.

4. Digital Safety, Wellbeing and Responsible Use	
DigComp 3.0 competencies	4.1 Protecting devices 4.2 Protecting personal data and privacy 4.3 Supporting well-being 4.4 Environmental impacts of digital technologies
Focus	Protecting devices, personal data, privacy, health, wellbeing and the environment in digital contexts.

4. Digital Safety, Wellbeing and Responsible Use	
Includes	Device protection and secure access; personal data and privacy management; digital wellbeing and harm reduction; environmental impacts of digital technologies and sustainability.

5. Digital Problem Identification and Solving	
DigComp 3.0 competencies	5.1 Identifying and solving technical problems 5.2 Identifying needs and digital technological responses 5.3 Identifying creative solutions using digital technologies 5.4 Identifying and addressing digital competence needs
Focus	Identifying needs and resolving problems through appropriate digital tools and approaches.
Includes	Solving technical problems; identifying digital technological responses to needs; creatively applying digital technologies; developing digital capability in self and others; designing for accessibility and inclusion.

Section 3 – Assessment Design and Contextualisation

3.1 Assessment Approach

All Digital Capability UoCs use the Application of Skills and Knowledge (ASK) template assessment structure. Assessment must be consistent with the Standards for RTOs 2025.

Performance Evidence must be demonstrated in a workplace or simulated workplace environment. Knowledge Evidence (KE) is assessed through structured questioning, written responses or other methods that confirm the candidate's understanding of the Knowledge items.

3.2 Simulated Assessment

Where direct workplace assessment is not practicable, assessment may be conducted in a simulated workplace environment consistent with the Assessment Conditions of the unit.

Simulation must reflect realistic workplace tools, contexts and constraints.

Level	Simulation requirements
Basic	Realistic workplace digital tools and scenarios under direct guidance; simulated workplace procedures; safe practice environment.
Intermediate	Realistic workplace digital tools and scenarios with limited supervision; varied scenario types; authentic workplace constraints (time, tools, requirements).
Advanced	Realistic workplace digital tools and scenarios requiring autonomous decision-making; varied and complex scenarios; authentic stakeholder dynamics.
Highly Advanced	Realistic workplace digital tools and scenarios requiring autonomy and accountability; complex multi-stakeholder scenarios; authentic accountability requirements.

DRAFT

Regulated sector simulation considerations

Regulated sector simulation considerations	
Health	Use de-identified clinical communication scenarios, simulated electronic health records, mock patient privacy scenarios; align with health information privacy and clinical governance requirements.
Early Childhood Education	Use simulated digital records (no real child data), mock parent communication scenarios; align with child safety and ECE digital practice standards.
Justice and Crime	Use de-identified case scenarios, simulated case management systems; align with privacy and security clearance requirements.
Defence	Use simulated environments meeting security clearance requirements; align with Defence cyber security and information handling standards.
Financial Services	Use de-identified client scenarios, simulated Customer Relationship Management (CRM) and reporting systems; align with privacy and financial services compliance requirements.
Education and Training	Use simulated student information systems with no real student data; align with student privacy and digital learning standards.

3.3 Foundation Skills in Assessment

Foundation skills are explicitly addressed in each unit per the TPOF standalone UoC requirements. Assessors should consider how foundation skill demands interact with assessment design, particularly for learners whose foundation skill levels may differ from the typical operating range of the unit.

Where foundation skill demands of an assessment task exceed a learner's current ACSF level, reasonable adjustment and/or flexibility to the assessment method may be appropriate.

Reasonable adjustment and/or flexibility must not reduce the standard required for competence.

Refer to Part B Section 2.3 for priority cohort guidance.

Foundation skill	Suggested assessment artefacts
Learning	Reflection journal entries; learning logs; progression pathway documentation.
Reading	Procedure interpretation tasks; policy summary tasks; technical document analysis; information evaluation tasks.
Writing	Workplace email composition; report writing; documentation of activities; summary of meetings or events.
Oral Communication	Recorded video calls; simulated client interactions; team meeting facilitation; verbal presentation of work.
Numeracy	Data summary tasks; basic KPI reporting; metrics interpretation; resource planning calculations.

DRAFT

3.4 Contextualisation

RTOs and employers may contextualise the Digital Capability UoCs to reflect specific industry settings, workplace tools, systems and terminology. Contextualisation must not remove or alter the learning outcomes, digital capability areas, or assessment requirements of the unit.

The following elements may be contextualised:

- Workplace tools and platforms – specific digital tools used in the industry or organisation
- Vocabulary and terminology – industry-specific language, acronyms and procedures
- Scenarios and examples – realistic workplace situations drawn from the relevant industry
- Assessment tasks – authentic workplace tasks that reflect industry practice.

Sector contextualisation examples

The following examples illustrate how the units can be contextualised for specific industries. These are examples only – RTOs should adapt to their specific workplace context.

Construction and Infrastructure	
Tools and platforms	Site management apps, project collaboration tools, mobile photo documentation, cloud-based drawing management.
Vocabulary	Site, supervisor, induction, Request for information (RFI), toolbox, scope, daily site diary, defect, handover, Workplace Health and Safety (WHS) digital reporting.

Health and Community Services	
Tools and platforms	Electronic health records (simulated), clinical communication tools, telehealth platforms, medication administration apps, secure messaging.
Vocabulary	Clinical handover, patient consent, clinical documentation, de-identification, mandatory reporting, duty of care.

Legal Services	
Tools and platforms	Legal research databases, case management systems, secure file sharing, e-discovery tools, court filing portals.
Vocabulary	Client confidentiality, conflict check, court filing, e-discovery, legal privilege, matter management.

Library Services	
Tools and platforms	Integrated library systems, digital catalogue tools, accessibility platforms, database subscriptions, digital collections management.
Vocabulary	Catalogue, ISBN, digital literacy, accessibility, inclusion, reference service, metadata.

DRAFT

Defence	
Tools and platforms	Secure messaging systems, classified document management, situational awareness tools (simulated), mission planning systems.
Vocabulary	Clearance, classification, OPSEC, brief, briefing pack, situational awareness, cyber hygiene.

Education and Training	
Tools	Learning management systems, student information systems, video conferencing, digital assessment tools, e-portfolio platforms.
Vocabulary	Cohort, learner, assessment, moderation, validation, RTO, AQF, AVETMISS, enrolment, training plan.

3.5 Example of Delivery Models

The Digital Capability UoCs support multiple delivery models. RTOs should select and combine delivery modes based on learner needs, industry context and available resources.

- **Standalone delivery:** UoCs delivered as discrete programmes, either face-to-face or online
- **Embedded delivery:** UoCs embedded within broader qualifications or programmes, with digital capability contextualised to the qualification's industry and purpose
- **Workforce uplift delivery:** UoCs delivered as part of an employer-commissioned digital capability uplift programme, typically at a single proficiency level across a workgroup
- **RPL and assessment-only:** assessment of existing digital capability without training delivery, using the evidence portfolio approach described in Part B Section 2.

3.6 Trainer and Assessor Capability

Trainers and assessors delivering the Digital Capability UoCs must meet the requirements of the Standards for RTOs 2025, including vocational competency and currency in the units they deliver and assess. For these UoCs, vocational competency and currency encompasses:

- Demonstrated digital capability at or above the proficiency level being delivered or assessed
- Currency in relevant digital tools, platforms and AI systems referenced in the UoCs Knowledge and Skills items
- Familiarity with the ASK template structure, including the relationship between Knowledge/Skills (K/S) items, Performance Evidence/Knowledge Evidence (PE/KE) blocks and Assessment Conditions
- For AI units: currency in AI tools and AI governance developments is particularly important given the pace of change in this domain.

3.7 Delivery of UoCs

Digital Capability units of competency can be delivered flexibly to suit different workforce needs and can be clustered together into a targeted training program addressing a specific capability gap. Clustering units from the same proficiency level and related competence areas allows RTOs to respond quickly to employer demand, for example: building AI and cyber security capability, or lifting digital communication and content creation skills without requiring learners to enrol in a full qualification. The suggested unit clusters below illustrate common combinations RTOs may consider; they are indicative as RTOs are able to design alternative combinations suited to their own industry context and learner cohort.

DRAFT

Suggested clustering

Skill set focus	Suggested unit cluster
Workforce Digital Capability - Core (any proficiency level)	Digital Skills in the workplace + 2 – 3 priority individual UoCs at the same proficiency level (targeted to a particular workforce need).
AI and Cyber Security at Work (Intermediate or Advanced)	AI + Cyber Security + Information Search + Digital Safety (4 units, same proficiency level).
Digital Communication and Content Creation (Intermediate or Advanced)	Communication and Collaboration + Content Creation + Information Search (3 units, same proficiency level).
Workforce Digital Capability - Refresh (cross-level progression)	Digital Skills In the Workplace at one level + selected individual units at the next level.

3.8 ASK Template

The ASK template is the unit format used by all Digital Capability UoCs. RTO trainers, assessors and learning designers familiar with the previous Elements and Performance Criteria (E&PC) format will find that ASK retains the same fundamental purpose: defining what learners must know, do, and demonstrate but expresses these requirements through a more contemporary and integrated structure.

Understanding the K + S → Application → KE/PE relationship

The ASK template separates four elements that work together:

- **Knowledge —** what learners need to understand (the conceptual basis for capability)
- **Skills —** what learners need to be able to do (the applied actions of capability)
- **Application of Knowledge and Skills —** how the knowledge and skills are applied in workplace contexts at the appropriate AQF level (autonomy, accountability, context, decision-making)
- **Performance Evidence and Knowledge Evidence —** what learners must demonstrate to be assessed as competent

Knowledge and Skills represent what is taught. Performance Evidence and Knowledge Evidence represent what is assessed. The Application section provides the AQF-level calibration that distinguishes one proficiency level from another.

Practical guidance for RTOs

When designing assessment for any of the Digital Capability UoCs:

- read the unit's Application section first — it defines the autonomy, accountability, context and decision-making expected at the proficiency level
- pitch assessment scenarios at the level described in Application — neither below nor above
- avoid scenarios that require sector-specific specialist content (for example, legal compliance frameworks, clinical protocols) unless they are illustrative of the digital capability being assessed
- keep digital capability the focus — sector context provides authenticity but should not become the assessment focus itself.

DRAFT

Part B: Implementation Guidance and Reference Materials

Section 1 – Digital Capability Area Reference

The tables below show, for each of the 32 Digital Capability UoCs, how each Digital Capability Area aligns to the unit's Knowledge, Skills, Performance Evidence and Knowledge Evidence.

Item numbers (K1, S1, PE1, KE1, etc.) are a referencing convention used only in this appendix, based on the sequential order in which items appear in each UoC, to support cross-referencing between the Digital Capability Areas and the unit's Knowledge, Skills, Performance Evidence and Knowledge Evidence. They do not appear in the endorsed UoC.

Performance Evidence and Knowledge Evidence are holistic assessment blocks and may, in some units, evidence more than one Digital Capability Area within a single item. Where this occurs, the item is listed against each area it evidences, with a note indicating the other area(s) covered.

Basic Level Units — BSBDIG201X–208X

BSBDIG201X — Develop Basic Digital Information Search, Evaluation and Management Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Browsing, searching and filtering information	K1: Factors affecting digital search results: search tool selection, privacy and security, and search terms entered. K2: Factors affecting variability and relevance of digital search results. K3: Main features of commonly used AI-driven and traditional digital search tools.	S1: Use digital search tools to conduct basic information searches. S2: Refine digital search results following established workplace procedures.	PE1: Conduct a digital search using workplace-approved tools to locate and access information relevant to a workplace task.	KE1: Digital search tools and the factors that affect the relevance and variability of workplace search results, including how AI-driven and traditional tools differ.
2. Evaluating information	K4: Differences between information sources and digital content. K5: Origins of digital content, human-generated or AI-generated.	S3: Follow established workplace fact-checking and verification procedures, under direct guidance, to check reliability and credibility of digital	PE2: Apply workplace fact-checking and verification procedures to determine whether located information is credible and relevant.	KE2: Digital information sources and content, sufficient to distinguish original from derived content, recognise AI-generated content, and

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	K6: Common examples of misinformation, disinformation and bias. K7: Social media influence and how digital platforms personalise content, including but not limited to filter bubbles.	information.		identify misinformation, disinformation, bias or platform personalisation.
3. Managing information	K8: Data removal, restoration and back-up functions. K9: Main properties of digital files and folders. K10: Common data types.	S4: Download, save, retrieve, move and delete digital files using workplace systems.	PE3: Organise, store and retrieve digital information using workplace-approved templates and systems.	KE3: Digital file and data management, including file and folder properties, common data types, and backup, restoration and removal procedures.

BSBDIG202X — Develop Basic Digital Communication and Collaboration Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Interacting through and with digital technologies	K1: Differences between synchronous and asynchronous digital communication, and between digital and non-digital interactions. K2: Basic features and functions of digital communication tools. K3: Key characteristics between human-to-human and human-to-machine interactions.	S1: Use basic features of digital communication tools to interact with individuals and groups under direct guidance.	PE1: Communicate with others using digital tools and platforms, both synchronously and asynchronously, to complete a workplace task.	KE1: Digital interaction methods, including how synchronous and asynchronous communication and human-to-machine interaction differ, and the features of digital communication tools available for a workplace task.
2. Sharing through digital technologies	K4: Benefits and risks of sharing information and content digitally. K5: Purpose, target audience, and appropriate channels for sharing	S2: Share information and content using established workplace procedures.	PE2: Share information or content securely through a digital channel appropriate to its purpose and audience.	KE2: Digital information sharing, including the benefits and risks of sharing content and how to match

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	information digitally.			audience and purpose to an appropriate digital channel.
3. Engaging in citizenship through digital technologies	K6: Examples of workplace and community participation online, and main purposes and functions of digital platforms and services. K7: Laws and regulations protecting the rights of users, and challenges that can impact digital exclusion of certain groups.	S3: Use digital platforms and services for routine workplace participation activities, following established workplace procedures.	PE3: Participate in a workplace or community activity using workplace-approved collaborative digital platforms and tools (also evidences Area 4, Collaborating).	KE3: Digital citizenship and participation, including workplace and community platforms, and the laws and factors that affect access and inclusion.
4. Collaborating through digital technologies	K8: Basic features and functions of digital collaboration tools.	S4: Participate in collaborative groups via digital tools under direct guidance.	PE3: (see Area 3 above — Participate in a workplace or community activity using workplace-approved collaborative digital platforms and tools).	KE4: Digital collaboration, including the features and functions of digital collaboration tools available for a workplace task.
5. Digital behaviour	K9: Differences in verbal and non-verbal behaviours in digital and non-digital contexts. K10: Online behaviours that may not be acceptable to others or may have legal consequences.	S5: Use tone and visual expression in formal and informal digital contexts following workplace guidelines.	PE4: Demonstrate appropriate tone and behaviour in a digital interaction and apply workplace procedures to manage digital identity (also evidences Area 6, Managing digital identity).	KE5: Digital behaviour, including differences between digital and non-digital verbal and non-verbal behaviour, and online behaviours that may be inappropriate or carry legal consequences.
6. Managing digital identity	K11: Features of physical and digital identities, including its dual function as authentication and as a record of online activities. K12: Persistence of internet information over time, digital footprints, and digital identity protection laws covering individuals' data and privacy.	S6: Follow workplace procedures to manage digital identity.	PE4: (see Area 5 above — Demonstrate appropriate tone and behaviour in a digital interaction and apply workplace procedures to manage digital identity).	KE6: Digital identity, including its dual function as authentication and behavioural record, the persistence of digital footprints, related privacy protections, and measures for managing digital identity.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	K13: Measures to manage digital identity.			

BSBDIG203X — Develop Basic Digital Content Creation Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Developing digital content	K1: Common types of digital content and their associated file formats. K2: Common operational functions across digital content creation tools. K3: The role of generative AI in supporting content creation, and the need for human oversight to ensure appropriate, accurate and context-relevant outputs.	S1: Use basic features of digital content creation tools to create and edit digital content in common formats. S2: Follow simple step-by-step sequences to produce digital content.	PE1: Create and edit a piece of digital content using workplace-approved tools, templates and established workplace procedures.	KE1: Digital content types, file formats, operational functions of common content creation tools, and the role of generative AI in supporting content creation with appropriate human oversight.
2. Integrating and adapting digital content	K4: Differences between editable and un-editable digital content. K5: Main functions of content creation tools for editing and integrating digital content.	S3: Apply basic editing, formatting and integration functions to modify existing digital content.	PE2: Modify and integrate existing digital content to meet workplace formatting and quality guidelines.	KE2: Digital content creation tools that support editing and integration of existing content, including the differences between editable and un-editable digital content.
3. Copyright and licences	K6: Copyright and licence concepts in digital contexts.	S4: Share digital content following basic legal and ethical guidelines.	PE3: Apply copyright, licensing and ethical guidelines when creating and sharing digital content for a workplace task.	KE3: Copyright and licence concepts that apply to the use and sharing of digital content.
4. Computational	K7: Common uses of automation	S5: Perform simple	PE4: Use an automation	KE4: Common workplace

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
thinking and programming	tools and computer applications in workplace contexts. K8: Common workplace AI applications and their basic functions.	repeatable tasks using basic automation features in workplace digital tools.	feature in a workplace digital tool to complete a routine content creation task.	automation tools, AI applications and the routine workplace tasks they support.

BSBDIG204X — Develop Basic Digital Safety, Wellbeing and Responsible Use Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Protecting devices	K1: Cyber security tools and everyday user actions that work together to protect a device. K2: Basic device protection measures, including antivirus software, screen locking, strong passwords, and multi-factor authentication. K3: Cyber security legislation that contributes to the security of digital products and services.	S1: Apply basic device protection measures following workplace procedures, including antivirus software, screen locking, strong passwords and multi-factor authentication.	PE1: Apply device protection measures, including a strong password and multi-factor authentication, following workplace procedures.	KE1: The role of cyber security tools, user actions and legislation in protecting workplace devices, including device protection measures such as antivirus software, screen locking, strong passwords and multi-factor authentication.
2. Protecting personal data and privacy	K4: Personal data collection generated through digital sources and processes, and the privacy rights that apply under legislation. K5: Risks associated with sharing personal data in digital environments. K6: Signs of identity theft.	S2: Respond to signs of identity theft following workplace procedures. S3: Block or flag personal information that has been shared inappropriately, following workplace procedures.	PE2: Protect personal data following workplace procedures, including responding to a security, privacy or identity concern as required.	KE2: Personal data collected and generated in digital environments, including privacy rights, privacy risks and indicators of identity theft.
3. Supporting wellbeing	K7: Main risks and benefits to physical, mental and social wellbeing in digital environments.	S4: Use workplace wellbeing guidelines to support personal digital habits.	PE3: Review and adjust personal digital habits using workplace wellbeing	KE3: The risks and benefits of digital technologies for physical, mental and social

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	K8: Digital platform features designed to capture and maintain attention, and limitations including risks of using virtual assistants and AI systems to support human wellbeing. K9: Strategies to support physical, mental and social wellbeing in digital environments, including signs and potential effects of problematic digital usage, and the role of laws and regulations in protecting wellbeing.		guidelines.	wellbeing, including attention-capturing platform design, the limitations of AI and virtual assistants, and strategies and protections that support wellbeing.
4. Environmental impacts of digital technologies	K10: Significant environmental impacts of some digital technologies and infrastructures. K11: The role of digital technologies in supporting energy efficiency and sustainability.	S5: Reduce energy and data consumption of digital technologies using simple strategies.	PE4: Adopt environmentally responsible practices for a workplace task involving digital technologies.	KE4: The environmental impacts of digital technologies and digital infrastructure, and the contribution of digital technologies to energy efficiency and sustainability.

BSBDIG205X — Develop Basic Digital Problem Identification and Solving Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Identifying and solving technical problems	K1: Differences between a device's operating system and the software applications used to perform work tasks. K2: Main features of common workplace digital devices, software applications, internet connectivity, and accessory devices.	S1: Follow instructions to resolve common technical problems. S2: Update software and applications following workplace procedures.	PE1: Identify a technical problem in a digital device or application and resolve it by following workplace procedures. PE2: Apply an update to software or an application in accordance with workplace	KE1: Common technical problems affecting workplace digital devices and applications, including the characteristics of operating system issues, software issues, and device or connectivity problems.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	K3: Signs of common technical problems.		procedures.	
2. Identifying user needs and matching digital technology responses	K4: Ways digital environments can be adjusted to meet user needs and preferences. K5: Purpose of digital assistance tools. K6: Common assistive technologies and their purposes.	S3: Adjust digital environment settings or features to meet user needs or preferences, following workplace procedures. S4: Use assistive technologies following workplace procedures. S5: Apply digital assistance tools to support simple tasks, following workplace guidelines on appropriate use.	PE3: Select and use a digital assistance tool or assistive technology to complete a workplace task, following workplace guidelines. PE4: Adjust digital environment settings to meet a specified user need or preference.	KE2: Digital assistance tools, assistive technologies and adjustable environment settings available to support workplace users.
3. Identifying creative solutions using digital technologies	K7: Examples of how a digital tool can be used in different ways to complete the same workplace task. K8: Basic benefits and limitations of using digital technologies to find alternative solutions to workplace tasks.	S6: Identify an alternative way a digital tool or application can be used to complete a workplace task. S7: Select and try a different digital approach or tool, following workplace guidance, when the usual method is not effective. S8: Explain, using a workplace example, how a digital technology can support problem-solving in a workplace task.	PE5: Identify and use an alternative digital tool or approach to complete a workplace task when the usual method is not effective. PE6: Explain, using a workplace example, how a digital technology supported the resolution of a workplace task.	KE3: Alternative digital approaches to completing workplace tasks, including the benefits and limitations of different tools and methods.
4. Identifying and addressing gaps in personal digital competence	K9: The scope of digital competence beyond technical skills. K10: The need for ongoing development of digital	S9: Recognise opportunities to improve personal digital competences and seek appropriate support when needed.	PE7: Review personal digital competence to identify at least one development need and an appropriate source of support.	KE4: Personal digital competence, and sources of support for identified development needs.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	competence for work, learning and daily life. K11: Opportunities to improve personal digital competences.			

BSBDIG206X — Develop Basic Digital Artificial Intelligence (AI) Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. AI and data awareness	K1: Processes used by AI systems to produce outputs from data. K2: Common AI applications and tools used in workplace contexts.	S1: Use approved AI tools following basic operating and quality verification procedures to complete routine workplace tasks.	PE1: Complete a routine workplace task using an approved AI tool, including verifying the AI-generated output against another source and recording or disclosing the AI contribution in line with workplace requirements (also evidences Area 2, Questioning AI output, and Area 5, Applied AI awareness).	KE1: AI systems, including their use of data to generate outputs, and common AI applications and tools used in workplace contexts.
2. Questioning AI output	K3: Recognition that AI outputs are suggestions or predictions and may need to be checked against other sources. K4: Recognition that AI-generated content can include synthetic media that may appear real.	S2: Check AI outputs using verification procedures, recognising that outputs are suggestions and predictions rather than confirmed facts.	PE1: (see Area 1 above — Complete a routine workplace task using an approved AI tool).	KE2: The limitations of AI-generated outputs, including the need to verify outputs against reliable sources, and the characteristics of AI-generated content, including synthetic media.
3. Understanding AI risks	K5: Common risks of AI use in workplace contexts: risks to safety, privacy, accuracy and fairness.	S3: Follow basic digital safety and privacy procedures including protection of sensitive information.	PE2: Demonstrate safe and lawful handling of data and sensitive information when using AI tools in accordance	KE3: Common risks associated with AI use in workplace contexts, including risks to safety,

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
			with workplace privacy and safety procedures.	privacy, accuracy and fairness.
4. Awareness of human-AI interaction	K6: Situations requiring human oversight when using AI tools, and limitations of AI that require human judgement.	S4: Respond to AI outputs that are unclear, inappropriate, harmful, or require human oversight, following workplace incident response and escalation procedures.	PE3: Respond appropriately to an AI output that is unclear, inappropriate, harmful, or requires human oversight by following workplace incident response and escalation procedures.	KE4: Situations requiring human oversight when using AI tools, including the limitations of AI that require human judgement.
5. Applied AI awareness	K7: Workplace requirements for disclosing AI use. K8: Workplace protocols and guidelines for selecting and using AI tools.	S5: Record AI use when required by workplace procedures, including but not limited to noting when AI tools have contributed to a task or output.	PE1: (see Area 1 above — Complete a routine workplace task using an approved AI tool).	KE5: Workplace requirements for disclosing the use of AI, and the protocols and guidelines for selecting and using AI tools.

BSBDIG207X — Develop Basic Digital Cyber Security Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Cyber security threat awareness	K1: Common workplace cyber security threats and their potential impact on workplace systems and information.	S1: Use established identification methods to recognise common workplace cyber security threats.	PE1: Recognise at least two common workplace cyber security threats encountered in routine workplace tasks, with reference to their likely impact on organisational systems or information.	KE1: Common workplace cyber security threats and their potential impact on workplace systems and information.
2. Workplace security protocols	K2: Workplace cyber security policies and procedures for protecting digital systems and information.	S2: Apply workplace security policies and procedures when using organisational digital systems.	PE2: Complete a routine workplace task using organisational digital systems in line with workplace	KE2: Workplace cyber security policies and procedures, including their role in protecting digital

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
			security policies and access controls.	systems and information.
3. Data protection	K3: Workplace security requirements for handling sensitive information securely: data classification, secure storage, appropriate sharing, and access controls.	S3: Handle workplace data securely in line with organisational data classification and protection requirements.	PE3: Handle at least one item of sensitive workplace information in accordance with organisational data classification, storage and sharing requirements.	KE3: The classification, storage, sharing and access control requirements for handling sensitive workplace information.
4. Incident response	K4: Workplace incident response procedures, including threat reporting requirements, escalation pathways and appropriate communication channels.	S4: Report cyber security threats and incidents through workplace channels.	PE4: Report a suspected cyber security threat or incident through the correct workplace channel, using appropriate communication and escalation pathways.	KE4: Workplace incident response procedures, including reporting requirements, escalation pathways and communication channels.
5. Security culture contribution	K5: The role of individual behaviours and practices in supporting workplace cyber security culture and organisational security objectives.	S5: Demonstrate security-conscious behaviours that support workplace cyber security practices.	PE5: Describe, using a workplace example, how individual practices and behaviours contribute to the organisation's cyber security culture.	KE5: Individual behaviours and practices that contribute to workplace cyber security culture and organisational security objectives.

DRAFT

BSBDIG208X — Develop Basic Digital Skills in the Workplace

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Information search, evaluation and management	K1: Digital search tools used to locate workplace information, and the criteria used to evaluate the reliability of search results. K2: The organisation and storage of digital files in workplace systems.	S1: Use digital search tools to locate workplace information and refine results following established workplace procedures. S2: Follow established workplace fact-checking and verification procedures to check reliability and credibility of digital information. S3: Organise and store digital files using basic workplace systems and templates, following workplace procedures.	PE1: Access, search, verify and organise workplace information using digital systems, and store files following workplace procedures.	KE1: Digital search tools used to locate workplace information, the criteria used to evaluate the reliability of search results, and the organisation and storage of digital files in workplace systems.
2. Communication and collaboration	K3: The features and uses of digital communication and collaboration tools relevant to workplace tasks. K4: Considerations for sharing information appropriately through digital channels.	S4: Use basic features of digital communication tools to interact with others. S5: Share information and content using digital platforms, following workplace procedures. S6: Participate in digital collaborative activities and follow established workplace procedures.	PE2: Participate in at least one workplace digital task that requires both interaction with others through workplace communication tools and contribution to a shared collaborative activity, applying organisational conventions for sharing information through digital channels.	KE2: The features and uses of digital communication and collaboration tools relevant to workplace tasks, and considerations for sharing information appropriately through digital channels.
3. Digital content creation	K5: Common digital content types and file formats, and the copyright and licensing requirements that apply to their use. K6: The use of generative AI to support content creation, and the	S7: Use basic features of content creation tools to create and edit digital content. S8: Apply basic formatting, editing and integration	PE3: Create and modify basic digital content using workplace tools and templates, in line with legal and ethical guidelines for using and sharing digital	KE3: Common digital content types, file formats and copyright and licensing requirements, including the use of generative AI to support content creation and

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	need for human oversight.	functions to existing digital content. S9: Share digital content following legal and ethical guidelines.	content.	the need for human oversight.
4. Safety, wellbeing and responsible use	K7: Basic device protection measures, including antivirus software, screen locking, strong passwords and multi-factor authentication. K8: The risks of sharing personal data digitally, and the risks and benefits of digital technology use for wellbeing.	S10: Implement basic device protection and security measures, including antivirus software, screen locking, strong passwords and multi-factor authentication, following workplace procedures. S11: Adopt simple strategies to support personal digital wellbeing.	PE4: Follow security, privacy and wellbeing practices for a workplace digital task.	KE4: Device protection measures, and the risks and benefits associated with sharing personal data and using digital technologies for wellbeing.
5. Problem identification and solving	K9: The basic features of hardware, software, connectivity and peripheral devices relevant to workplace tasks. K10: Common technical issues in workplace digital environments, and the purpose of digital assistance tools.	S12: Follow instructions to resolve common technical problems. S13: Draw on digital assistance tools, following workplace guidelines, to support simple workplace tasks.	PE5: Recognise and resolve at least one common technical problem encountered during a workplace digital task, drawing on established troubleshooting procedures, available digital assistance tools, and escalation pathways.	KE5: Hardware, software, connectivity and peripheral devices relevant to workplace tasks, common technical issues in workplace digital environments, and the purpose of digital assistance tools.

DRAFT

Intermediate Level Units — BSBDIG301X–308X

BSBDIG301X — Develop Intermediate Digital Information Search, Evaluation and Management Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Browsing, searching and filtering information	K1: Strategies for distinguishing between relevant and less relevant digital search results, and for improving search relevance.	S1: Select appropriate digital search tools based on information needs. S2: Translate information needs into effective digital search queries, commands or statements. S3: Refine or filter search results or outputs using appropriate strategies.	PE1: Resolve a workplace information need of moderate complexity by selecting and applying appropriate digital search tools, strategies and filters to obtain relevant results.	KE1: Strategies for distinguishing relevant from less relevant digital search results and improving search relevance.
2. Evaluating information	K2: Potential consequences of misinformation and disinformation in digital environments. K3: Methods for identifying the source of online information, and the purpose of fact-checking services. K4: How bias in training data can lead to inaccurate AI system outputs. K5: Examples of human bias in information generation and human interpretation, and the importance of ethical considerations. K6: Human responsibility for checking the quality and validity of AI-generated information and content. K7: How digital platforms and content can influence user choices and behaviours.	S4: Apply strategies to identify and disregard unreliable sources and content. S5: Recognise and respond appropriately to digital platforms or content that may influence user choices and behaviours. S6: Evaluate the reliability of sources and content, including AI systems, personalised content and commercial or other interests.	PE2: Determine the credibility and reliability of digital information and content, including AI-generated content, by identifying sources, applying fact-checking techniques and recognising bias or misinformation, to support a workplace task.	KE2: Methods for verifying online sources and content, including fact-checking; the causes and ethical implications of misinformation, disinformation and bias, including AI and human bias; and the influence of digital platforms and AI-generated content on user choices, including the responsibility to verify AI content before use.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
3. Managing information	K8: Methods for renaming, organising, saving and transferring digital files and folders across devices, external storage and cloud services. K9: Common data collection tools, their main functions, and associated responsibilities including lawful data handling. K10: Common data types and formats.	S7: Apply naming conventions to digital files and folders. S8: Save, manage and delete files across digital devices, external storage and cloud services. S9: Manage information within digital accounts. S10: Use data collection tools for simple data processing. S11: Organise, format and apply basic formulas to data in structured digital environments.	PE3: Organise, manage and process digital information and data for a workplace task, using file naming conventions, folder structures, multiple storage locations, and data collection tools and basic formulas in structured digital environments.	KE3: File and data management practices for organising, storing and transferring digital files across devices, external storage and cloud services, and the functions and lawful handling responsibilities associated with common data collection tools and data types.

BSBDIG302X — Develop Intermediate Digital Communication and Collaboration Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Interacting through and with digital technologies	K1: Range of digital interaction tools used in workplace contexts. K2: Contexts in which asynchronous, synchronous, or non-digital communication is most effective.	S1: Select suitable digital and non-digital communication tools for given contexts and use multiple features to interact with and manage individuals, groups and channels. S2: Develop and refine prompts for AI systems to support routine digital interactions, with appropriate disclosure and attribution of AI-generated content.	PE1: Communicate for a workplace task using digital tools selected for context and purpose, including synchronous and asynchronous channels. PE2: Develop prompts for AI system interactions, with appropriate disclosure and attribution, and share information ethically for a workplace task, including assessing risks and reporting misinformation through appropriate channels (also	KE1: The range of digital interaction and communication tools used in workplace contexts, and the contexts in which synchronous, asynchronous or non-digital communication is most effective.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
			evidences Area 2, Sharing).	
2. Sharing through digital technologies	K3: Responsibilities and effective ethical practices for sharing information and content in digital environments.	S3: Identify risks, benefits and ethical implications when sharing information, and report misinformation and disinformation through workplace channels.	PE2: (see Area 1 above — Develop prompts for AI system interactions, with appropriate disclosure and attribution, and share information ethically for a workplace task...).	KE2: The responsibilities and ethical practices that apply to sharing information and content in digital environments.
3. Engaging in citizenship through digital technologies	K4: Ways to participate in workplace and community activities through digital technologies. K5: Use of digital platforms and services in workplace and community activities, with associated benefits and risks.	S4: Engage with digital platforms and services to share information and resources, considering opportunities, risks and ethical implications within workplace contexts.	PE3: Participate in a workplace or community activity using digital platforms and services, considering the risks and benefits of their use.	KE3: Ways to participate in workplace and community activities through digital platforms and services, including the associated benefits and risks.
4. Collaborating through digital technologies	K6: Features and functions of digital collaboration tools, including human-AI collaboration.	S5: Select digital collaboration tools aligned to collaboration goals, and create, manage and effectively contribute to simple collaborative tasks.	PE4: Coordinate and contribute to a collaborative task using selected digital tools, including ethical human-AI collaboration.	KE4: The features and functions of digital collaboration tools, including human-AI collaboration.
5. Digital behaviour	K7: Rights and responsibilities relating to digital behaviour, and the relationship between digital behaviour and digital reputation.	S6: Use respectful and inclusive tone and visual expression in formal and informal digital environments.	PE5: Demonstrate respectful and inclusive digital behaviour appropriate to formal and informal contexts and diverse audiences.	KE5: The rights and responsibilities associated with digital behaviour, and its relationship to digital reputation.
6. Managing digital identity	K8: Relationships between digital footprint, reputation and identity, and ways to check the scope of own digital identity. K9: Features and functions used to	S7: Adjust settings on devices, applications and online accounts to manage own digital identity across platforms, in line with	PE6: Manage own digital identity across multiple platforms for a workplace context, including adjusting settings and checking digital	KE6: The relationship between digital footprint, reputation and identity, and the features used to check and manage digital identity.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	manage digital identity.	workplace expectations.	footprint scope.	

BSBDIG303X — Develop Intermediate Digital Content Creation Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Developing digital content	K1: Benefits, limitations and ethical considerations in the use of digital technologies for content creation. K2: Strategies that support efficient digital content creation including but not limited to templates and appropriate sequencing of tasks.	S1: Create and edit digital content across multiple formats using a range of digital content creation tools. S2: Identify audience needs, including inclusivity and accessibility requirements, and apply appropriate adjustments.	PE1: Create and edit digital content across multiple formats using a range of tools, for a defined audience and addressing accessibility needs.	KE1: The benefits, limitations and ethical considerations of using digital technologies for content creation, and strategies that support efficient content creation such as templates and task sequencing.
2. Integrating and adapting digital content	K3: Structure, format and audience requirements of digital content integration or adaptation tasks. K4: Ethical and transparent practices in digital content integration and adaptation, acknowledging re-used digital content, and disclosure and attribution of AI-generated content from generative AI systems.	S3: Adjust, integrate or transform digital content to meet format, structure and audience requirements. S4: Modify or transform digital textual, numeric or visual representations to accurately convey meaning. S5: Enhance or integrate existing digital content using digital technologies selectively, ethically and transparently, including appropriate disclosure and attribution of AI-generated content.	PE2: Modify, integrate and adapt existing digital content for a workplace task, using AI systems ethically and disclosing AI-generated content.	KE2: The structure, format and audience requirements for content integration and adaptation tasks, including ethical and transparent practices such as acknowledging re-used content and disclosing AI-generated content.
3. Copyright and licences	K5: Intellectual property concepts in digital contexts including but	S6: Apply legal and ethical guidelines appropriately	PE3: Use and share digital content for a workplace task	KE3: Intellectual property concepts including

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	not limited to copyright, trademark, design and patent. K6: Common licence types and purposes in digital contexts. K7: Examples of plagiarism in digital contexts, where copyright applies, and the legal, ethical and commercial consequences of intellectual property violations.	when using, re-using and sharing digital content.	in line with copyright, licensing and intellectual property requirements.	copyright, trademark, design and patent, common licence types, and the legal, ethical and commercial consequences of plagiarism and intellectual property violations.
4. Computational thinking and programming	K8: Algorithm concepts, the general steps in computational thinking, and basic programming concepts. K9: Common programming languages and automation tools, and their range of potential workplace applications. K10: How machine learning is applied, selected and verified in workplace automation and AI systems.	S7: Recognise steps in routine workplace processes that could be supported by automation tools, using computational thinking. S8: Configure simple automation features available in workplace digital tools, applying basic logic and control structures. S9: Create visual representations including but not limited to flowcharts to illustrate routine workplace processes or basic algorithms.	PE4: Apply computational thinking to a routine workplace process, creating a visual representation of the process or a basic algorithm, and identifying automation opportunities.	KE4: Computational thinking and algorithm concepts, common programming languages and automation tools, and how machine learning is applied, selected and verified in workplace automation and AI systems.

DRAFT

BSBDIG304X — Develop Intermediate Digital Safety, Wellbeing and Responsible Use Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Protecting devices	K1: The use of AI systems in cyber-attacks and cyber security. K2: Main features and functions of privacy tools: passwords, two-factor authentication, and access controls.	S1: Protect devices and their contents using prevention techniques, including passwords, two-factor authentication and access controls.	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.	KE1: The use of AI systems in both cyber-attacks and cyber security, and the features and functions of privacy tools such as passwords, two-factor authentication and access controls.
2. Protecting personal data and privacy	K3: Key underlying concepts of data protection and privacy legislation, and the complexity of personal data ownership in AI systems. K4: Privacy implications of online content sharing, and its use in AI training.	S2: Manage personal data and privacy across varied digital environments, including effective use of privacy tools.	PE2: Manage personal data and privacy for a workplace task, using privacy tools such as passwords, two-factor authentication or access controls.	KE2: Data protection and privacy legislation concepts, including the complexity of personal data ownership in AI systems and the privacy implications of sharing content online and its use in AI training.
3. Supporting wellbeing	K5: Reliable information sources and inclusive groups or communities that support physical, mental and social wellbeing. K6: Examples of harmful digital content and behaviour, their impacts, and how digital technologies, particularly social media, can amplify bias, stereotyping and exclusion. K7: Strategies to protect against, or respond to, harmful behaviour or content when encountered.	S3: Review and adapt personal digital usage patterns to support physical, mental and social wellbeing. S4: Implement strategies to protect against, and respond effectively to, harmful behaviour and content.	PE3: Review digital usage patterns to support physical, mental and social wellbeing, and implement strategies to protect against and respond to harmful behaviour or content.	KE3: Reliable sources of wellbeing support, and how harmful digital content and behaviour, including bias, stereotyping and exclusion amplified through digital technologies can be recognised and responded to.
4. Environmental impacts of digital technologies	K8: Environmental impacts of digital technologies across manufacturing, usage and	S5: Reduce environmental impacts of digital technology use through strategies	PE4: Apply environmental sustainability strategies throughout the device	KE4: The environmental impacts of digital technologies across

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	disposal: data centres, e-commerce, and AI systems. K9: How digital tools can support sustainable living. K10: Collaborative consumption concepts and strategies for extending device lifecycles, including their associated risks, limitations and environmental benefits.	including device purchasing, usage, repair, recycling and disposal.	lifecycle, including informed purchasing, usage, repair and disposal decisions, and considering environmental impacts of AI systems.	manufacturing, use and disposal, including data centres, e-commerce and AI systems, and how digital tools, collaborative consumption and lifecycle-extension strategies can support sustainable living.

BSBDIG305X — Develop Intermediate Digital Problem Identification and Solving Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Identifying and solving technical problems	K1: Common causes of technical problems in digital devices and applications, and indicators that signal when a device or system is not performing as expected. K2: A range of human-assisted and technology-assisted strategies for troubleshooting technical problems in digital environments.	S1: Troubleshoot technical problems in digital environments using varied human-assisted and technology-assisted strategies. S2: Update and adjust settings on main and peripheral digital devices to maintain performance.	PE1: Troubleshoot a technical problem in a digital environment for a workplace task, using human-assisted or technology-assisted strategies. PE2: Update and adjust digital device settings to maintain performance and meet workplace requirements.	KE1: Common causes of technical problems in digital devices and applications, the indicators that signal an issue, and human-assisted and technology-assisted troubleshooting strategies.
2. Identifying needs and digital technological responses	K3: The concept of human-centric design and its role in the development and use of digital technologies.	S3: Adjust digital environment features to suit personal and others' needs and preferences. S4: Select digital assistance tools to support needs, with awareness of their benefits and limitations.	PE3: Adjust digital environment features and use digital assistance tools to support diverse needs, recognising benefits and limitations.	KE2: The concept of human-centric design and its role in the development and use of digital technologies to meet user needs.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
3. Identifying creative solutions using digital technologies	K4: Examples of interactions between humans and digital technologies in creativity and problem-solving. K5: The strengths, limitations and ethical considerations of digital technologies in supporting human creativity and problem-solving.	S5: Identify strengths and limitations of digital technologies in relation to specific problem-solving tasks. S6: Engage with digital technologies responsibly and ethically to support individual or group problem-solving.	PE4: Identify strengths and limitations of digital technologies for specific problem-solving tasks, and use them responsibly and ethically, individually or in groups.	KE3: Examples of interaction between humans and digital technologies in creativity and problem-solving, and the associated strengths, limitations and ethical considerations.
4. Identifying and addressing digital competence needs	K6: Relevant learning opportunities to meet personal digital competence needs.	S7: Review own digital competence and identify development needs.	PE5: Review own digital competence for a workplace role and identify relevant learning opportunities to address any gaps.	KE4: Learning opportunities relevant to addressing personal digital competence needs.

BSBDIG306X — Develop Intermediate Digital Artificial Intelligence (AI) Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. AI and data in action	K1: The processes used by AI systems to generate outputs from structured and unstructured data. K2: Systematic approaches for selecting AI tools based on task requirements, data compatibility, and output needs.	S1: Select AI tools appropriate to workplace tasks based on data requirements and output needs. S2: Apply AI tools to complete routine tasks while managing data inputs according to workplace procedures, including lawful data handling requirements.	PE1: Use at least two different AI tools systematically to complete routine workplace tasks.	KE1: How AI systems process structured and unstructured data to generate outputs, and systematic approaches for selecting AI tools based on task requirements.
2. Evaluating AI output	K3: Criteria used to evaluate AI-generated outputs, including accuracy, relevance, fairness, bias, authenticity and workplace quality requirements.	S3: Evaluate AI-generated outputs against workplace criteria and authoritative sources or benchmarks for accuracy, relevance, fairness	PE2: Evaluate AI outputs, identify limitations, bias and synthetic or manipulated content, and apply verification procedures.	KE2: Criteria, methods and verification procedures used to evaluate AI-generated outputs for accuracy, relevance, fairness, bias and

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	K4: Methods for detecting bias, fairness concerns, inconsistencies, limitations, and synthetic or manipulated content in AI-generated outputs. K5: Verification procedures used to validate AI outputs against authoritative sources and workplace standards.	and authenticity. S4: Identify limitations, bias and synthetic or manipulated content in AI outputs using systematic checking and verification processes.		authenticity against authoritative sources and workplace requirements.
3. Managing AI risks	K6: Workplace protocols for managing AI-related risks including but not limited to privacy protection, data security, lawful data handling, record-keeping, incident response and escalation procedures. K7: Approaches for identifying and addressing bias through systematic verification and quality control processes.	S5: Implement AI risk management protocols, including privacy, data security, lawful data handling and record-keeping requirements. S6: Apply bias and fairness identification procedures and follow incident response and escalation procedures when required.	PE3: Implement AI risk management protocols, including privacy, data security, lawful data handling and incident response measures.	KE3: Workplace protocols for managing AI-related risks, including privacy, security, lawful data handling, incident response, and systematic approaches for identifying and addressing bias.
4. Human-AI collaboration	K8: Workflows integrating human judgement with AI capabilities, with transitions between human and AI tasks, quality control, and human oversight for complex or sensitive information.	S7: Coordinate human judgement with AI assistance, establishing appropriate transitions between human and AI tasks and quality control measures. S8: Apply human oversight for decisions with workplace consequences and where contextual judgement is required.	PE4: Coordinate human judgement with AI capabilities, including transitions between human and AI tasks and quality control measures.	KE4: Workflows for integrating human judgement with AI capabilities, including transitions between human and AI tasks, quality control and oversight of complex or sensitive information.
5. AI integration	K9: The integration of AI tools within workplace systems and workflows, and performance measures for assessing AI	S9: Integrate AI tools into workplace procedures, including disclosure and attribution of AI-generated	PE5: Integrate AI tools into workplace procedures, including disclosure and attribution of AI-generated	KE5: Methods for integrating AI tools within workplace systems, performance measures for assessing AI

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	effectiveness through productivity and quality outcomes. K10: Workplace requirements for disclosing and attributing AI-generated content.	content, while maintaining compatibility and performance standards. S10: Monitor AI performance and implement adjustments to improve effectiveness and quality.	content, while maintaining performance and verification standards.	effectiveness, and workplace requirements for disclosing and attributing AI-generated content.

BSBDIG307X — Develop Intermediate Digital Cyber Security Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Cyber security threat awareness	K1: Common workplace cyber security threats (including but not limited to AI-enhanced threats, phishing and social engineering) and their potential impact on organisational operations.	S1: Recognise common workplace cyber security threats and suspicious activities.	PE1: Recognise and respond to at least two different common workplace cyber security threats using established procedures.	KE1: The nature of common workplace cyber security threats, including AI-enhanced threats, and their potential impact on organisational operations.
2. Workplace security protocols	K2: Workplace security procedures and protocols used to protect digital systems, devices, and information in routine workplace contexts.	S2: Apply workplace security procedures and protocols to protect digital systems, devices, and information.	PE2: Apply workplace security procedures to protect digital systems, devices and information for a workplace task.	KE2: The role of workplace security procedures and protocols in protecting digital systems, devices and information.
3. Data protection	K3: Workplace requirements for protecting sensitive information including but not limited to access controls, secure storage methods, and appropriate data handling procedures.	S3: Protect sensitive workplace information by applying access controls, appropriate data handling procedures and using secure storage methods.	PE3: Apply appropriate access controls, secure storage methods and data handling procedures to protect sensitive workplace information for a workplace task.	KE3: The requirements for protecting sensitive workplace information, including access controls, secure storage and data handling procedures.
4. Incident	K4: Workplace procedures for	S4: Report security concerns	PE4: Report at least one	KE4: The steps and decision

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
response participation	reporting security concerns, escalating incidents and participating in incident response activities.	and incidents through appropriate workplace channels.	security concern and incident through appropriate workplace channels and participate in response activities.	points involved in reporting, escalating and participating in workplace incident response.
5. Security culture contribution	K5: Approaches for supporting workplace cyber security awareness and promoting secure workplace practices.	S5: Support workplace security awareness by sharing security knowledge with colleagues.	PE5: Contribute to a workplace security awareness activity or share security knowledge with at least one colleague to support a positive workplace security culture.	KE5: The contribution of individual security awareness practices to a positive workplace cyber security culture.

BSBDIG308X — Develop Intermediate Digital Skills in the Workplace

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Information search, evaluation and management	K1: Search strategies for improving relevance of digital results, evaluation of source credibility and AI system limitations. K2: Approaches for organising digital files across devices, external storage and cloud services.	S1: Select appropriate digital search tools and translate information needs into effective digital search queries. S2: Apply strategies to identify and discard unreliable sources and content. S3: Apply naming conventions and folder hierarchies, and manage files across devices, external storage and cloud services.	PE1: Conduct and document targeted information searches, including the criteria used to evaluate source credibility and the organisation of information for workplace use.	KE1: Search strategies for improving the relevance of digital results, methods for evaluating source credibility and recognising AI system limitations, and approaches for organising digital files across devices, external storage and cloud services.
2. Communication	K3: Features and functions of	S4: Select communication	PE2: Coordinate, contribute	KE2: The features and

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
and collaboration	digital communication and collaboration tools, AI-enabled functionalities and ethical human-AI collaboration, and appropriate use contexts. K4: Ethical responsibilities for sharing information, digital participation in workplace and community activities, and key rights and responsibilities under digital laws and regulations.	tools suited to varied contexts and use multiple features to interact with individuals and groups. S5: Identify risks, benefits and ethical implications of sharing information, and report misinformation and disinformation. S6: Select collaboration tools aligned to goals, create and manage simple collaborative tasks, and contribute effectively.	to and document digital communication and collaboration activities across at least two tools or platforms, demonstrating ethical information sharing and appropriate responses to misinformation, disinformation and risks.	functions of digital communication and collaboration tools, including AI-enabled functionalities and ethical human-AI collaboration, the ethical responsibilities for sharing information, and key rights and responsibilities under digital laws and regulations.
3. Digital content creation	K5: Benefits, limitations and ethical considerations of using digital technologies for content creation. K6: Structure, format and audience requirements for digital content integration and adaptation. K7: Intellectual property concepts in digital contexts, and computational thinking and algorithm concepts.	S7: Create and edit digital content across multiple formats using a range of tools. S8: Identify inclusivity and accessibility requirements and edit content to meet audience needs. S9: Interact with AI systems purposefully and ethically to support content creation, including disclosure and attribution of AI-generated content. S10: Apply legal and ethical guidelines when using and sharing digital content.	PE3: Create and edit at least two digital content items across different formats, edited to meet accessibility and audience requirements, with evidence of ethical AI interaction, including disclosure and attribution of AI-generated content where applicable, and application of intellectual property principles.	KE3: The benefits, limitations and ethical considerations of using digital technologies for content creation, structure, format and audience requirements for integration and adaptation, and related intellectual property and computational thinking concepts.
4. Safety, wellbeing and responsible use	K8: Key concepts of cyber security, including types of threats, protective practices, AI-enhanced threats and AI cyber security	S11: Apply prevention techniques to protect devices and data, including using passwords, two-factor	PE4: Implement security threat prevention and privacy measures for a workplace task, and review, adapt and	KE4: Key cyber security and data protection concepts, including AI-enhanced threats and applications,

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	applications, and the data protection and privacy legislation that governs organisational and personal responsibilities. K9: Sources of wellbeing support, impacts of harmful content and behaviour, and environmental impacts of digital technologies including but not limited to data centres, e-commerce and AI systems.	authentication and access controls. S12: Manage personal data and privacy across digital environments using appropriate tools. S13: Review and adapt personal digital usage patterns to support wellbeing. S14: Implement strategies to respond to harmful behaviour and content.	record digital usage in response to wellbeing considerations and harmful content.	sources of wellbeing support, the impacts of harmful content and behaviour, and the environmental impacts of digital technologies.
5. Problem identification and solving	K10: Human-centric design principles, and the strengths, limitations and ethical considerations of digital technologies in supporting human creativity and problem-solving.	S15: Troubleshoot technical problems using human-assisted and technology-assisted strategies and adjust digital environment features to meet personal and others' needs, including informed use of digital assistance tools.	PE5: Resolve at least one technical problem using human-assisted or technology-assisted strategies, with adjustments of digital environment settings to meet personal or others' needs.	KE5: Human-centric design principles and the strengths, limitations and ethical considerations of digital technologies in supporting human creativity and problem-solving.

DRAFT

Advanced Level Units — BSBDIG401X–408X

BSBDIG401X — Develop Advanced Digital Information Search, Evaluation and Management Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Browsing, searching and filtering information	K1: Advanced search functions and features of familiar and emerging digital search tools.	S1: Critically evaluate advanced functions and features of familiar and emerging digital search tools for complex, non-routine information tasks. S2: Combine multiple search tools and strategies to address information requirements.	PE1: Resolve a complex, non-routine information need by combining multiple search tools and strategies, critically evaluating advanced search functions to select the most appropriate approach. PE4: Coach a colleague to strengthen their capability in digital search, evaluation or information management (this coaching item applies across all three digital capability areas of this unit).	KE1: Advanced search functions and features of familiar and emerging digital search tools, and their appropriate application to workplace information needs.
2. Evaluating information	K2: Personal, social and political consequences of misinformation, disinformation, bias and social media influence. K3: Characteristics of trustworthy digital technologies and methods for identifying artificially generated or manipulated digital content. K4: Potential sources of error, inaccuracy or bias in information and data.	S3: Analyse how AI systems, bias and vested interests influence digital information creation and presentation. S4: Systematically assess the reliability, accuracy and credibility of diverse digital sources using multiple validation methods.	PE2: Establish the reliability, accuracy and credibility of digital information affected by AI systems, bias or vested interests, applying multiple validation methods to a source with conflicting or uncertain evidence. PE4: (see Area 1 above — Coach a colleague to strengthen their capability in digital search, evaluation or information management).	KE2: The personal, social and political consequences of misinformation, disinformation, bias and social media influence, the indicators of trustworthy digital technologies, methods for identifying artificially generated or manipulated content, and the potential sources of error, inaccuracy or bias in information and data.
3. Managing information	K5: Approaches to managing, processing and analysing digital information and data across workplace contexts.	S5: Apply ethical, transparent, lawful and secure information management practices.	PE3: Apply ethical, transparent, lawful and secure information management practices to	KE3: Key steps in managing, processing and analysing digital information and data, and the characteristics,

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	K6: Features of open data and big data: applications, benefits and limitations.	S6: Identify, analyse and mitigate potential sources of error, inaccuracy or bias in data collection, management and processing. S7: Use advanced functions and a range of tools and methods to transfer, organise, process and analyse digital information. S8: Interpret information to inform workplace decision-making.	organise and analyse a complex or ambiguous dataset, identifying and mitigating sources of error or bias, to inform a workplace decision. PE4: (see Area 1 above — Coach a colleague to strengthen their capability in digital search, evaluation or information management).	applications, benefits and limitations of open data and big data.

BSBDIG402X — Develop Advanced Digital Communication and Collaboration Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Interacting through and with digital technologies	K1: Factors influencing effective digital communication across diverse organisational contexts. K2: Approaches for developing and refining AI prompts to achieve communication outcomes.	S1: Combine communication tools to address complex tasks across varied contexts, coordinating complex digital events where required. S2: Develop and refine prompts for AI systems to handle complex interactions.	PE1: Address a complex communication task by combining and coordinating appropriate digital communication tools, including for a complex digital event. PE2: Develop and refine AI prompts to handle a complex interaction, sharing the resulting information ethically to support professional goals (also evidences Area 2, Sharing).	KE1: Factors influencing effective digital communication across diverse organisational contexts, and approaches for developing and refining AI prompts to achieve communication outcomes.
2. Sharing through	K3: Principles governing ethical	S3: Share information	PE2: (see Area 1 above —	KE2: The principles governing

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
digital technologies	information sharing in professional environments (including but not limited to disclosure and attribution of AI-generated content).	ethically to support professional goals, guiding a colleague in ethical information sharing practices.	Develop and refine AI prompts to handle a complex interaction, sharing the resulting information ethically to support professional goals).	ethical information sharing in professional environments, including disclosure and attribution of AI-generated content.
3. Engaging in citizenship through digital technologies	K4: High-risk and prohibited AI systems under legislation, with potential societal, political or economic impacts.	S4: Assess digital technologies for inclusion and democratic impacts, applying this assessment to support others to participate and exercise their digital rights.	PE3: Assess a digital technology for inclusion, exclusion or democratic impact, including analysis of a high-risk AI system, and support a colleague to participate and exercise their digital rights.	KE3: High-risk and prohibited AI systems under legislation, and their potential societal, political or economic impacts.
4. Collaborating through digital technologies	K5: Approaches for effective human-AI collaboration in workplace contexts.	S5: Select collaboration tools to meet project needs, ensuring ethical AI use and assessing the effectiveness of human-AI collaboration. S9: Coach a colleague to develop capability in digital collaboration or identity management.	PE5: (see Area 6 below — Manage digital identity across multiple environments, coaching a colleague to develop their digital collaboration or identity management capability).	KE4: Approaches for effective human-AI collaboration in workplace contexts.
5. Digital behaviour	K6: Ethical, legal and illegal behaviours in digital environments. K7: Types of abuse in digital environments, affected groups, potential impacts, obligations and ways to report and respond to abuse.	S7: Respond effectively to difficult digital situations, promoting inclusive behaviour within a team or work area. S8: Evaluate ethical and legal aspects of digital behaviour, analysing patterns and impacts of digital abuse.	PE4: Respond to a difficult or contested digital behaviour situation, applying ethical and legal analysis and promoting inclusive behaviour.	KE5: Ethical, legal and illegal behaviours in digital environments, including types of digital abuse, affected groups, impacts, and obligations to report and respond.
6. Managing digital	K8: Digital identity management,	S9: Manage digital identity	PE5: Manage digital identity	KE6: Digital identity

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
identity	associated rights, and the use of AI systems in identity management.	across multiple environments, assessing AI implications and curating identities for varied purposes.	across multiple environments, coaching a colleague to develop their digital collaboration or identity management capability (also evidences Area 4, Collaborating).	management, associated rights, and the use of AI systems in identity management.

BSBDIG403X — Develop Advanced Digital Content Creation Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Developing digital content	K1: Factors influencing selection of content creation tools and methods for workplace tasks. K2: Principles of accessibility and usability in advanced digital content creation.	S1: Select and combine digital content creation tools and methods to meet complex content and audience requirements. S2: Create and edit complex or specialised digital content tailored to defined goals and audiences.	PE1: Produce accessible, complex or specialised digital content by selecting and combining appropriate creation tools and methods, tailored to defined goals and audiences. PE4: Refine digital content based on an evaluation against defined quality, accessibility and usability criteria and stakeholder feedback.	KE1: Factors influencing the selection of content creation tools and methods for workplace tasks, and the principles of accessibility and usability in advanced digital content creation.
2. Integrating and adapting digital content	K3: Methods used for complex digital content integration and adaptation. K4: Appropriate and inappropriate uses of AI systems to enhance digital content integration or adaptation in complex tasks considering risks of synthetic	S3: Adjust and integrate diverse digital content to meet complex format, structure and audience requirements. S4: Use digital technologies selectively, ethically and transparently to achieve	PE2: Integrate and adapt digital content to meet complex format, structure or audience requirements, applying copyright, licensing and intellectual property guidelines where relevant (also evidences Area 3,	KE2: Methods for complex digital content integration and adaptation, including the appropriate and inappropriate use of AI systems and the risks of synthetic media and AI-generated manipulation.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	media and AI-generated manipulation.	integration or adaptation.	Copyright and licences).	
3. Copyright and licences	K5: Key features of current legislation relating to digital copyright and licences, with examples of application and exclusions in digital contexts. K6: Differences in how ethical and copyright issues apply to AI training data and AI-generated content and disclosure and attribution requirements.	S5: Apply legal and ethical requirements for using and sharing digital content in complex contexts.	PE2: (see Area 2 above — Integrate and adapt digital content to meet complex format, structure or audience requirements, applying copyright, licensing and intellectual property guidelines where relevant).	KE3: Current legislation relating to digital copyright and licences, including its application and exclusions, and how ethical and copyright issues differ between AI training data and AI-generated content.
4. Computational thinking and programming	K7: Human-centric approaches in programming and AI systems including human oversight, user experience and customer experience. K8: Approaches for selecting, applying and verifying automation tools or AI systems. K9: Main types of machine learning, and the features and purposes of commonly used machine learning algorithms. K10: Routine tasks suitable for partial or full automation using automation tools or AI systems.	S6: Evaluate ethical and practical considerations in the development and deployment of computer programmes and AI systems. S7: Draw on computational thinking to develop automated solutions for routine workplace tasks and computational problems using automation tools or AI systems. S8: Coach a colleague to develop capability in digital content creation, integration or adaptation, including legal and ethical application.	PE3: Evaluate the ethical and practical considerations of using, deploying or automating AI systems in a content creation or integration task. PE5: Coach a colleague to develop capability in ethical and responsible digital content creation, integration or computational thinking (this coaching item also evidences Area 1 and Area 2).	KE4: Human-centric approaches to programming and AI systems, including human oversight, the steps for selecting, applying and verifying automation tools or AI systems, the main types and purposes of machine learning algorithms, and the routine tasks suited to partial or full automation.

DRAFT

BSBDIG404X — Develop Advanced Digital Safety, Wellbeing and Responsible Use Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Protecting devices	K1: Rights of individuals under current cyber security legislation. K2: The use of recent and emerging technologies in cyber-attacks and cyber security.	S1: Update cyber security measures to protect devices and their contents in response to evolving digital threats. S2: Coach a colleague to implement device protection measures and understand their rights under data protection and privacy legislation.	PE1: Update and prioritise cyber security measures in response to an evolving digital threat, coaching a colleague to implement device protection measures.	KE1: The key rights of individuals under current cyber security legislation, and how recent and emerging technologies, including AI, are used in cyber-attacks and cyber security.
2. Protecting personal data and privacy	K3: Data protection and privacy rights under current legislation, with associated strategies for protecting personal data and managing privacy in digital environments.	S3: Implement strategies to protect personal data and manage privacy in digital environments.	PE2: Support a colleague to understand their rights under data protection and privacy legislation, while implementing personal data protection and privacy management strategies.	KE2: Data protection and privacy rights under current legislation, and associated strategies for protecting personal data and managing privacy in digital environments.
3. Supporting wellbeing	K4: Wellbeing and inclusion rights in digital environments. K5: Approaches for identifying and responding to harmful behaviour, content and deceptive design, particularly AI-generated content and synthetic media.	S4: Facilitate reviews of digital technology usage with individuals and teams to support physical, mental and social wellbeing. S5: Flag or intervene effectively in instances of harmful behaviour, content or deceptive design in digital environments. S6: Build the capability of others to recognise and counter digital technologies that reinforce bias, stereotyping and exclusion.	PE3: Facilitate a review of digital technology usage with an individual or team to support physical, mental or social wellbeing, and identify or respond to an instance of harmful behaviour, content or deceptive design. PE4: Build the capability of others to recognise and counter digital technologies that reinforce bias, stereotyping or exclusion.	KE3: Wellbeing and inclusion rights in digital environments, and approaches for identifying and responding to harmful behaviour, content and deceptive design, particularly involving AI-generated content and synthetic media.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
		S7: Communicate and reinforce wellbeing and inclusion rights in digital environments across varied workplace contexts.		
4. Environmental impacts of digital technologies	K6: Environmental impacts of digital technologies (including but not limited to energy and resource demands of AI training and operation) and strategies for reducing environmental impact of digital technology use.	S8: Evaluate environmental impacts of digital technologies to inform decision-making or advocacy. S9: Advise a colleague on assessing their digital technology use and identifying opportunities to reduce environmental impact.	PE5: Evaluate the environmental impacts of digital technologies to inform a decision or advocacy position, advising a colleague on opportunities to reduce their environmental impact.	KE4: The environmental impacts of digital technologies, including the energy and resource demands of AI training and operation, and strategies for reducing environmental impact.

BSBDIG405X — Develop Advanced Digital Problem Identification and Solving Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Identifying and solving technical problems	K1: Advanced solution-finding strategies for troubleshooting technical problems and diagnostic approaches for digital environment issues.	S1: Apply advanced strategies to troubleshoot technical problems in digital environments. S2: Coach a colleague to diagnose and resolve technical problems in digital environments.	PE1: Troubleshoot a technical problem in a digital environment using advanced strategies, coaching a colleague to diagnose and resolve a related issue.	KE1: Advanced solution-finding strategies and diagnostic approaches for troubleshooting technical problems in digital environments.
2. Identifying needs	K2: Methods for assessing	S3: Adjust digital	PE2: Adjust digital	KE2: Methods for assessing

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
and digital technological responses	accessibility, inclusivity, fairness and rights-sensitivity of digital technologies. K3: Approaches for configuring digital environments to meet diverse needs.	environment features to meet diverse user needs and preferences, evaluating the effectiveness of configurations and digital assistance tools. S4: Assess the accessibility, inclusivity, fairness and rights-sensitivity of digital technologies in context.	environment features to meet diverse user needs, assessing the accessibility, inclusivity, fairness and rights-sensitivity of the resulting configuration.	the accessibility, inclusivity, fairness and rights-sensitivity of digital technologies, and approaches for configuring digital environments to meet diverse needs.
3. Identifying creative solutions using digital technologies	K4: Principles underpinning human-centric, ethical and responsible digital problem-solving. K5: Creative approaches for applying digital technologies to non-routine problems.	S5: Use digital technologies efficiently, responsibly and ethically to solve problems, prioritising human-centric approaches. S6: Contribute to initiatives that apply digital technologies to problem-solving tasks.	PE3: Apply digital technologies efficiently, responsibly and ethically to a non-routine problem, contributing to an initiative that applies digital technologies to problem-solving.	KE3: The principles underpinning human-centric, ethical and responsible digital problem-solving, and creative approaches for applying digital technologies to non-routine problems.
4. Identifying and addressing digital competence needs	K6: Approaches for monitoring digital technological developments and competence implications. K7: Strategies for coaching and supporting others to develop confidence, autonomy and digital capability. K8: Sources, methods and criteria for identifying, compiling and contextualising digital competence learning opportunities.	S7: Monitor digital technological developments and their implications for digital competence needs, engaging in ongoing self-development. S8: Compile and contextualise digital competence learning opportunities to build another person's confidence, capability and autonomy in digital environments.	PE4: Monitor digital technological developments relevant to your own competence needs, and compile learning opportunities to build another person's confidence, capability and autonomy.	KE4: Approaches for monitoring digital technological developments and their competence implications, strategies for coaching and supporting others to develop digital capability, and sources and methods for compiling learning opportunities.

DRAFT

BSBDIG406X — Develop Advanced Digital Artificial Intelligence (AI) Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Applying AI and data practices	K1: Approaches for implementing AI systems in non-routine workplace contexts.	S1: Implement AI applications across workplace processes, including AI tools introduced to support existing tasks. S2: Demonstrate AI applications and share structured approaches to promote practical AI use among colleagues.	PE1: Implement AI-enabled solutions using at least three different AI tools across a workplace process.	KE1: Approaches for implementing AI systems in non-routine workplace contexts.
2. Challenging AI output	K2: Methods and criteria for assessing AI outputs and system performance. K3: Frameworks for identifying bias, fairness considerations, inconsistency, error and synthetic media risks in AI-generated results.	S3: Evaluate AI outputs and system performance using defined quality criteria, identifying limitations and biases through systematic evaluation. S4: Advise a colleague on assessment strategies, including verification procedures and evaluation criteria.	PE2: Evaluate AI outputs and system performance against defined quality criteria, identifying and addressing limitations, bias, inconsistency or error.	KE2: Methods for assessing AI outputs and system performance, and frameworks for identifying bias, fairness considerations, inconsistency, error and synthetic media risks in AI-generated results.
3. Applying responsible AI practices	K4: Ethical AI practices and risk management approaches applicable to organisational contexts (disclosure and attribution of AI-generated content, lawful data handling, consequential decision thresholds, and auditable records of AI use).	S5: Apply ethical AI practices, privacy controls, security measures and vendor or tool assurance considerations in workplace contexts. S6: Address AI adoption risks, supporting a colleague in risk identification.	PE3: Apply ethical AI principles, data governance requirements and privacy controls to manage AI-related risks in a workplace context, including incident identification and response.	KE3: Ethical AI practices and risk management approaches applicable to organisational contexts, including disclosure and attribution of AI-generated content, lawful data handling, consequential decision thresholds, and auditable records of AI use.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
4. Coordinating human-AI collaboration	K5: Strategies for optimising collaboration between people and AI systems. K6: Approaches for supporting and guiding others to work effectively with AI tools.	S7: Coordinate effective human-AI collaboration by embedding appropriate human oversight. S8: Coach a colleague to optimise human-AI partnerships while maintaining critical thinking.	PE4: Coordinate effective human-AI collaboration in a workplace task, embedding appropriate human oversight and verification. PE5: (see Area 5 below — Support AI adoption that builds sustainable organisational capability, coaching a colleague to optimise human-AI partnerships and collaborative effectiveness).	KE4: Strategies for optimising collaboration between people and AI systems, and approaches for guiding and supporting others to work effectively with AI tools.
5. Applied AI integration in workplace processes	K7: Methods for implementing AI tools within workplace processes. K8: Strategies for enabling sustainable organisational AI adoption, including environmental impact considerations associated with AI training and operation.	S9: Integrate AI tools within workplace processes, aligning AI use with organisational objectives and building capability in others.	PE5: Support AI adoption that builds sustainable organisational capability, coaching a colleague to optimise human-AI partnerships and collaborative effectiveness (also evidences Area 4, Coordinating human-AI collaboration).	KE5: Methods for implementing AI tools within workplace processes, and strategies for enabling sustainable AI adoption, including the environmental impact of AI training and operation.

BSBDIG407X — Develop Advanced Digital Cyber Security Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Cyber security threat assessment	K1: The use of emerging technologies used in cyber-attacks and cyber security. K2: Approaches for identifying, analysing and evaluating cyber	S1: Identify and analyse cyber security threats and vulnerabilities in workplace contexts, evaluating risk levels using appropriate methods.	PE1: Identify and assess at least three different cyber security threats in a workplace context, evaluating risk levels and advising a	KE1: Emerging technologies used in cyber-attacks and cyber security, and approaches for identifying, analysing

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	security threats and vulnerabilities in workplace contexts.		colleague on appropriate protective responses.	and evaluating cyber security threats and vulnerabilities in workplace contexts.
2. Security implementation	K3: Methods for implementing security measures and maintaining secure systems.	S2: Determine and implement protective practices to maintain secure environments, monitoring their effectiveness through systematic checking.	PE2: Implement, monitor and systematically review security measures across workplace systems to maintain a secure environment.	KE2: Methods for implementing security measures and maintaining secure systems.
3. Data protection and privacy	K4: Data protection and privacy requirements (including security controls, access management and compliance considerations).	S3: Coordinate data protection initiatives using appropriate security controls, maintaining privacy standards across systems and processes. S4: Manage access controls and compliance requirements.	PE3: Protect workplace data and maintain privacy standards, ensuring compliance and coordinating data protection initiatives.	KE3: Data protection and privacy requirements, including security controls, access management and compliance considerations.
4. Incident response coordination	K5: Incident response procedures, recovery processes and stakeholder communication approaches.	S5: Implement and coordinate incident response and recovery activities during security events. S6: Coach a colleague to strengthen incident management capability.	PE4: Coordinate a cyber security incident response and recovery activity, communicating with stakeholders during the security event and reviewing outcomes to identify improvements to incident management capability.	KE4: Incident response procedures, recovery processes and stakeholder communication approaches.
5. Security culture development	K6: Strategies for promoting security awareness and building organisational security culture.	S7: Promote security awareness and mitigation strategies in workplace contexts. S8: Contribute to initiatives that build organisational security culture.	PE5: Contribute to a programme or initiative that builds sustainable cyber security awareness and culture in a workplace context.	KE5: Strategies for promoting security awareness and building organisational security culture.

DRAFT

BSBDIG408X — Develop Advanced Digital Skills in the Workplace

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Information search, evaluation and management	K1: Personal, social and political consequences of misinformation, disinformation, bias and social media influence. K2: Characteristics of trustworthy digital technologies and methods for identifying deep-fakes and AI-generated synthetic media. K3: Sources of error or inaccuracy in digital information and processes for managing, processing and analysing digital information and data. K4: Features, applications, benefits and limitations of open data and big data.	S1: Integrate advanced digital search tools and strategies to address complex information needs. S2: Assess the reliability and accuracy of diverse sources, including AI-generated content and bias, to support workplace decisions. S3: Coach a colleague to develop advanced information search and evaluation capability.	PE1: Implement advanced information search and evaluation methods, assessing diverse sources including AI-generated content and bias, to support a workplace decision.	KE1: The personal, social and political consequences of misinformation, disinformation, bias, social media influence, the indicators of trustworthy digital technologies and methods for identifying deep-fakes and AI-generated synthetic media, sources of error or inaccuracy in digital information, and the features, applications, benefits and limitations of open data and big data.
2. Communication and collaboration	K5: Ethical, legal and illegal behaviours in digital environments, and types of digital abuse, affected groups, impacts, and reporting mechanisms. K6: Relationship between technological development and digital identity management.	S4: Combine communication and collaboration tools for complex tasks, guiding a colleague in tool selection. S5: Share information ethically, advising a colleague on ethical digital communication practices. S6: Evaluate digital technologies for inclusion, supporting a colleague to understand and exercise their digital rights.	PE2: Coordinate ethical digital communication and collaboration using integrated tools, supporting a colleague to build their digital collaboration capability. PE7: Support a colleague to understand and exercise their digital rights, contributing to their integrated digital capability development (also evidences Area 5, Problem identification and solving).	KE2: Ethical, legal and illegal behaviours in digital environments, including types of digital abuse, affected groups, impacts and reporting mechanisms, and the relationship between technological development and digital identity management.
3. Digital content	K7: High-risk and prohibited AI	S7: Select digital content	PE3: Create specialised digital	KE3: High-risk and prohibited

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
creation	systems, human-centric approaches and oversight principles, and types, features and purposes of common machine-learning approaches and algorithms. K8: Methods for complex digital content integration and adaptation including appropriate and inappropriate AI use. K9: Copyright and licensing legislation, including distinctions between AI training data and AI-generated content.	creation tools to produce specialised content aligned to defined goals and audiences. S8: Apply ethical, transparent AI use and legal guidelines to a content integration or adaptation task. S9: Use computational thinking and automation tools or AI systems to automate a routine workplace task.	content using ethical AI practices and legal guidelines. PE4: Use automation tools or AI systems, applying computational thinking to automate a routine workplace task.	AI systems, human-centric approaches and oversight principles, methods for complex digital content integration and adaptation including appropriate and inappropriate AI use, and copyright and licensing legislation as it applies to AI training data and AI-generated content.
4. Safety, wellbeing and responsible use	K10: Rights under cyber security legislation and the use of emerging technologies, including AI, in cyber-attacks and cyber security.	S10: Implement and update cyber security measures, coaching a colleague to apply protection strategies. S11: Manage privacy and wellbeing risks, intervening in a harmful situation where required. S12: Monitor the environmental impacts of digital technologies, supporting sustainable practice.	PE5: Apply cyber security, privacy, wellbeing and sustainability practices in a workplace context.	KE4: Rights under cyber security legislation and the use of emerging technologies, including AI, in cyber-attacks and cyber security.
5. Problem identification and solving	K11: Advanced diagnostic and solution-finding strategies for resolving technical problems. K12: Principles underpinning human-centric, ethical and rights-sensitive digital problem-solving, including approaches for evaluating accessibility, inclusivity	S13: Diagnose and resolve a technical problem using solution-finding strategies, evaluating the accessibility, inclusivity, fairness and rights-sensitivity of the resulting solution. S14: Track digital	PE6: Diagnose and resolve a technical problem using human-centric approaches, evaluating the accessibility, inclusivity, fairness, rights-sensitivity and democratic impact of the resulting solution.	KE5: Advanced solution-finding strategies for diagnosing and resolving technical problems, the principles underpinning human-centric, ethical and rights-sensitive digital problem-solving, and

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	and fairness. K13: Approaches for monitoring digital technological developments and supporting capability development in self and others.	technological developments relevant to your own competence needs and support another person's ongoing capability development.	PE7: (see Area 2 above — Support a colleague to understand and exercise their digital rights, contributing to their integrated digital capability development).	approaches for monitoring digital technological developments and supporting capability development in self and others.

Highly Advanced Level Units — BSBDIG501X–508X

BSBDIG501X — Develop Highly Advanced Digital Information Search, Evaluation and Management Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Browsing, searching and filtering information	K1: Emerging developments in digital search technologies and their applications.	S1: Select and apply advanced search methods to novel or highly complex information problems that fall outside standard approaches. S2: Combine multiple advanced search tools and strategies to resolve information needs spanning several workplace functions. S3: Take responsibility for the technical quality of search and evaluation work completed by others, providing expert guidance where approaches are unclear.	PE1: Resolve a complex workplace information need by selecting, combining and applying advanced search methods and tools, and by taking responsibility for the technical quality of related work completed by others. PE4: Provide expert advice or mentoring that builds another person's information search, evaluation or management capability (this coaching item applies across all three digital capability areas of this unit).	KE1: Emerging developments in digital search technologies and their practical applications to complex workplace information tasks.
2. Evaluating information	K2: Methods for information validation, quality assessment and	S4: Critically analyse how AI systems, bias and vested	PE2: Establish the reliability and credibility of information	KE2: Methods for validating information, assessing its

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	credibility analysis. K3: Approaches for promoting resilience to misinformation and disinformation.	interests shape the information landscape, and apply this analysis to atypical or contested cases. S5: Apply a wide range of validation methods to establish the reliability, accuracy and credibility of information in situations involving conflicting or incomplete evidence. S6: Contribute specialist expertise to organisational efforts to build resilience to misinformation and disinformation.	in a situation involving conflicting, incomplete or contested evidence, applying multiple validation methods and critically accounting for the influence of AI systems, bias or vested interests. PE4: (see Area 1 above — Provide expert advice or mentoring that builds another person's information search, evaluation or management capability).	quality and credibility, and building organisational resilience to misinformation and disinformation.
3. Managing information	K4: Advanced tools and methods for data management, processing and analysis. K5: Approaches for structuring, documenting and applying governance frameworks to workplace data and information. K6: Approaches for leading capability development across digital information competencies.	S7: Apply advanced governance and documentation frameworks to structure and secure complex or sensitive datasets, within established organisational policy. S8: Apply advanced analytical tools and methods, including big data techniques, to complex or ambiguous datasets, transferring techniques from other contexts where needed. S9: Provide expert advice and mentoring to build the information search, evaluation and management capability of others.	PE3: Apply governance, documentation and analytical frameworks, including big data techniques where relevant, to manage a complex or sensitive dataset within established organisational policy. PE4: (see Area 1 above — Provide expert advice or mentoring that builds another person's information search, evaluation or management capability).	KE3: Advanced tools and methods for managing, processing and analysing data, the governance frameworks used to structure and document workplace data and information, and approaches for building organisational capability in digital information competencies.

DRAFT

BSBDIG502X — Develop Highly Advanced Digital Communication and Collaboration Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Interacting through and with digital technologies	K1: Emerging developments in communication technologies.	S1: Select and combine communication tools and approaches to resolve complex, non-routine workplace communication challenges. S2: Take responsibility for the quality of communication practice across a team or work area, refining tools and methods as new technologies emerge.	PE1: Resolve a complex, non-routine communication challenge by selecting and combining appropriate tools and methods, and by taking responsibility for the quality of communication practice within a team or work area.	KE1: Emerging developments in communication technologies, and approaches for applying communication practices to complex workplace contexts.
2. Sharing through digital technologies	K2: Approaches for facilitating and improving complex information sharing across varied digital technologies.	S3: Resolve complex or ambiguous information-sharing problems by adapting methods across multiple, varied digital technologies.	PE2: Address an information-sharing problem spanning multiple digital technologies, adapting methods to fit varied or unfamiliar platforms.	KE2: Approaches for facilitating and improving complex information sharing across varied digital technologies.
3. Engaging in citizenship through digital technologies	K3: Legislative requirements relating to digital citizenship.	S4: Interpret how digital technologies affect society, political processes and the economy, and apply this understanding to workplace decisions involving digital citizenship. S5: Provide expert guidance to colleagues on their legislative rights and responsibilities relating to digital citizenship.	PE3: Analyse the impact of a digital technology on society, political processes or the economy, and apply this analysis to a workplace decision involving digital citizenship, including advising a colleague on their legislative rights and responsibilities.	KE3: Legislative requirements relating to digital citizenship, their application in workplace contexts, and approaches for embedding compliant practice.
4. Collaborating through digital	K4: Emerging developments in collaborative tools.	S6: Apply ethical and proportionate AI use in	PE4: Apply ethical and proportionate AI use to a	KE4: Emerging developments in

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
technologies	K5: Ethical and proportionate use of AI in communication and collaboration. K6: Approaches for developing and applying collaboration practices in complex workplace contexts.	collaborative work, adapting collaborative approaches to complex or unfamiliar environments. S7: Take responsibility for the quality of human-AI collaboration within a team or work area.	collaborative task in a complex or unfamiliar environment, taking responsibility for the quality of the resulting human-AI collaboration.	collaborative tools, the principles of ethical and proportionate AI use in collaboration, and approaches for applying collaboration practices to complex workplace contexts.
5. Digital behaviour	K7: Emerging developments in digital behaviour legislation. K8: Legislative requirements relating to digital behaviour.	S8: Critically evaluate new and existing digital behaviour policies and legislation, applying this analysis to atypical or contested situations. S9: Provide expert guidance to colleagues on their rights and responsibilities under digital behaviour legislation.	PE5: Evaluate a digital behaviour policy or piece of legislation as it applies to an atypical or contested situation and advise a colleague on their rights and responsibilities under digital behaviour legislation.	KE5: Emerging developments in digital behaviour legislation and its legislative requirements.
6. Managing digital identity	K9: Emerging developments in identity management systems. K10: Legislative requirements relating to identity management. K11: Approaches for building capability in others across digital communication, collaboration, behaviour and identity management.	S10: Apply specialist knowledge of emerging identity management technologies to resolve complex identity management or rights issues. S11: Provide expert advice and mentoring to build another person's identity management capability.	PE6: Draw on specialist knowledge of emerging identity management technologies to resolve a complex identity management or rights issue, and mentor another person to build their identity management capability.	KE6: Emerging developments in identity management systems, associated legislative requirements, and approaches for building organisational capability across digital communication, collaboration, behaviour and identity management.

DRAFT

BSBDIG503X — Develop Highly Advanced Digital Content Creation Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Developing digital content	K1: Emerging developments in content creation tools, platforms and technologies. K2: Approaches for developing and applying content practices, quality standards and accessibility requirements across complex workplace contexts.	S1: Select and apply advanced design and data visualisation techniques to produce content for complex or unfamiliar organisational purposes. S2: Take responsibility for the quality and accessibility of content produced by a team or work area, applying inclusive design principles to atypical requirements. S8: Evaluate the effectiveness of content against organisational objectives, accessibility requirements and user needs, and identify improvements within established frameworks.	PE1: Produce content for a complex or unfamiliar organisational purpose by applying advanced design and data visualisation techniques and take responsibility for the quality and accessibility of related work completed by others. PE5: Evaluate content against organisational objectives, accessibility requirements and user needs, and implement an improvement within established frameworks.	KE1: Emerging developments in content creation tools, platforms and technologies, and approaches for applying content practices and quality standards to complex workplace tasks.
2. Integrating and adapting digital content	K3: Approaches for applying content integration methods in complex workplace contexts.	S3: Resolve complex content integration problems by adapting methods across varied platforms and formats. S4: Take responsibility for the technical quality of content integration work completed by others, providing expert guidance where approaches are unclear.	PE2: Adapt methods across varied platforms to resolve a complex content integration problem, providing expert guidance where the approach is unclear.	KE2: Approaches for applying content integration methods to complex workplace requirements.
3. Copyright and licences	K4: Copyright, licensing and intellectual property requirements in digital environments.	S5: Apply specialist knowledge of copyright, licensing and intellectual property requirements to resolve complex or ambiguous content use questions.	PE3: Resolve a complex or ambiguous copyright, licensing or intellectual property question, and advise a colleague on requirements relevant to their work.	KE3: Copyright, licensing and intellectual property requirements that apply to digital content.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
		S6: Provide expert guidance to colleagues on copyright, licensing and intellectual property requirements relevant to their work.		
4. Computational thinking and programming	K5: Ethical use of automation tools and responsible AI practices. K6: Approaches for developing organisational capability and embedding continuous improvement across content creation, integration and automation.	S7: Apply ethical and transparent automation and AI practices to complex content creation tasks, evaluating new tools and applications as they emerge. S9: Provide expert advice and mentoring to build another person's content creation or integration capability.	PE4: Apply ethical and transparent automation or AI practices to a complex content creation task, evaluating the suitability of an emerging tool or application.	KE4: Ethical automation and responsible AI practices, and approaches for building organisational capability across content creation, integration and automation tools.

BSBDIG504X — Develop Highly Advanced Digital Safety, Wellbeing and Responsible Use Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Protecting devices	K1: Emerging developments in cyber security technologies. K2: Legislative and regulatory frameworks for cyber security. K3: Methods for developing cyber security initiatives. K4: Ethical and responsible use of digital technologies including governance principles and risk management.	S1: Interpret and apply cyber security legislation to resolve complex or ambiguous compliance questions. S2: Take responsibility for the quality of device and content protection practices across a team or work area.	PE1: Address a complex or ambiguous cyber security compliance question by interpreting relevant legislation and take responsibility for the quality of device and content protection practices within a team or work area.	KE1: Emerging developments in cyber security technologies, associated legislative and regulatory frameworks, and methods for developing cyber security initiatives that reflect ethical, governance and risk management principles.
2. Protecting	K5: Emerging developments in	S3: Apply specialist knowledge	PE2: Apply specialist	KE2: Emerging developments

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
personal data and privacy	data protection and privacy solutions. K6: Legislative and regulatory frameworks for data protection. K7: Methods for developing data protection approaches.	of data protection and privacy regulatory frameworks to resolve complex data protection problems. S4: Provide expert advice on data protection approaches within established organisational policy.	knowledge of data protection regulatory frameworks to a complex data protection problem, providing expert advice within established organisational policy.	in data protection and privacy solutions, associated legislative and regulatory frameworks, and methods for developing data protection approaches.
3. Supporting wellbeing	K8: Legislative and regulatory frameworks for wellbeing. K9: Methods for developing wellbeing programs.	S5: Evaluate wellbeing and inclusion evidence to resolve complex or contested workplace situations. S6: Provide expert guidance to colleagues on embedding wellbeing and inclusion into digital systems and practices. S7: Contribute specialist expertise to legal and regulatory considerations relating to digital wellbeing and inclusion.	PE3: Evaluate evidence to address a complex or contested wellbeing or inclusion issue and provide expert guidance to a colleague on embedding wellbeing and inclusion into digital systems or practices.	KE3: Legislative and regulatory frameworks for wellbeing, and methods for developing workplace wellbeing programs.
4. Environmental impacts of digital technologies	K10: Emerging developments in environmental sustainability impacts. K11: Legislative and regulatory frameworks for sustainability. K12: Approaches for building capability in others across digital safety, wellbeing and sustainability.	S8: Apply specialist knowledge of environmental and sustainability impacts to resolve complex sustainability problems in digital technology use. S9: Provide expert advice and mentoring to build another person's capability in sustainable and responsible digital technology use.	PE4: Draw on specialist knowledge of environmental impacts to resolve a complex sustainability problem in digital technology use, and mentor another person to build their capability in sustainable and responsible use.	KE4: Emerging developments in environmental sustainability impacts, associated legislative and regulatory frameworks, and approaches for building organisational capability across digital safety, wellbeing and sustainability.

DRAFT

BSBDIG505X — Develop Highly Advanced Digital Problem Identification and Solving Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Identifying and solving technical problems	K1: Methods for developing and delivering training to support digital device and system use.	S1: Resolve complex technical problems using digital technologies and build confidence and autonomy in others to do the same. S2: Design and deliver training that builds another person's capability to use digital devices and systems effectively.	PE1: Resolve a complex technical problem using digital technologies, taking responsibility for the quality of related problem-solving practice within a team or work area. PE4: Design and deliver training or learning materials that build another person's digital device, system or competence capability, while monitoring and addressing your own development needs (also evidences Area 4, Identifying and addressing digital competence needs).	KE1: Methods for developing and delivering training that builds digital device and system capability in others.
2. Identifying needs and digital technological responses	K2: Methods for evaluating and contributing to improvements in digital assistance tools and accessible technologies. K3: Approaches for promoting inclusive and accessible digital technologies. K4: Methods for assessing complex needs and tailoring digital solutions.	S3: Apply specialist knowledge of inclusive and accessible digital technologies to resolve complex accessibility problems. S4: Assess complex or ambiguous user needs and tailor digital solutions accordingly. S5: Contribute specialist expertise to improving digital assistance tools and accessible technologies.	PE2: Resolve a complex accessibility or user-needs problem by applying specialist knowledge of inclusive and accessible digital technologies and contribute to improving a digital assistance tool or accessible technology.	KE2: Methods for evaluating and improving digital assistance tools and accessible technologies, approaches for promoting inclusive and accessible design, and methods for assessing complex needs to tailor digital solutions.
3. Identifying creative solutions	K5: Approaches for leading initiatives that apply digital	S6: Apply digital technologies to develop innovative	PE3: Apply digital technologies to develop an	KE3: Approaches for leading initiatives that apply digital

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
using digital technologies	technologies to complex problem-solving in workplace contexts.	responses to complex, unfamiliar problem-solving challenges. S7: Take responsibility for the quality of problem-solving practice within a team or work area.	innovative response to an unfamiliar or complex problem-solving challenge.	technologies to complex workplace problem-solving.
4. Identifying and addressing digital competence needs	K6: Approaches for mentoring others in digital competence development and developing learning materials.	S8: Monitor personal development needs and engage in ongoing self-development to maintain complex digital competence. S9: Provide expert mentoring and develop learning materials to build another person's digital competence.	PE4: (see Area 1 above — Design and deliver training or learning materials that build another person's digital device, system or competence capability, while monitoring and addressing your own development needs).	KE4: Approaches for mentoring others in digital competence development, and methods for developing supporting learning materials.

BSBDIG506X — Develop Highly Advanced Digital Artificial Intelligence (AI) Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. AI and data optimisation	K1: Decision-making principles for selecting and applying AI approaches.	S1: Select and apply AI approaches to resolve complex, non-routine organisational challenges. S2: Take responsibility for the quality of AI use and integration within a team or work area.	PE1: Resolve a complex, non-routine organisational challenge by selecting and applying appropriate AI approaches, taking responsibility for the quality of AI use and integration within a team or work area.	KE1: Decision-making principles applied when selecting and applying AI approaches to workplace tasks.
2. AI output evaluation	K2: Governance frameworks for AI system evaluation and output quality assessment.	S3: Apply and contribute to frameworks for evaluating AI system performance and	PE2: Evaluate AI system performance and outputs for bias, error and synthetic	KE2: Governance frameworks used to evaluate AI systems and assess the quality of AI

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
		output quality. S4: Assess AI outputs for bias, error and synthetic media risks, applying governance requirements including disclosure and audit trail considerations. S5: Address governance requirements spanning privacy, security, bias, synthetic media, vendor assurance and regulatory considerations.	media risks, applying governance frameworks addressing privacy, security, vendor assurance and regulatory considerations.	outputs.
3. AI risk management	K3: Ethical AI practices, risk management approaches and accountability mechanisms including disclosure, audit and incident response considerations.	S6: Navigate ethical AI practices and risk management approaches in complex or ambiguous situations, contributing to organisational policies and practices.	PE3: Apply ethical AI practices and risk management approaches to a complex or ambiguous situation, contributing to organisational policies and practices for responsible AI use.	KE3: Ethical AI practices, risk management approaches and accountability mechanisms, including disclosure, audit and incident response considerations.
4. Human-centred AI practice	K4: Human-centred AI design principles that maintain critical thinking and effective collaboration.	S7: Design human-centred AI approaches that maintain appropriate oversight and preserve critical thinking. S8: Integrate human judgement with AI capabilities to navigate complex or competing organisational priorities. S9: Provide expert advice and mentoring to build another person's understanding of effective human-AI collaboration.	PE4: Integrate human judgement with AI capabilities to navigate a task requiring oversight and critical thinking, applying human-centred AI approaches.	KE4: Human-centred AI design principles that maintain critical thinking and effective human-AI collaboration.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
5. AI integration and capability development	K5: Organisational capability development approaches for AI adoption. K6: Methods for adopting and integrating AI while maintaining ethical standards.	S10: Draw on specialist knowledge to integrate AI tools within workplace processes, contributing to organisational capability development for AI adoption.	PE5: Provide expert advice or mentoring that builds another person's capability to integrate AI tools within workplace processes.	KE5: Organisational capability development approaches for AI adoption, and methods for adopting and integrating AI while maintaining ethical standards.

BSBDIG507X — Develop Highly Advanced Digital Cyber Security Skills

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Security awareness and threat recognition	K1: Emerging developments in cyber security technologies and threat intelligence. K2: Methods for implementing and maintaining threat management systems. K3: Ethical and proportionate application of cyber security practices and technologies. K4: Legislative and regulatory frameworks relating to cyber security.	S1: Critically evaluate cyber security technologies, threat intelligence and evolving threat landscapes to inform workplace decisions. S2: Develop and apply integrated threat management approaches that draw on security intelligence and emerging technologies.	PE1: Address a complex or evolving cyber security threat by developing and applying integrated threat management approaches that draw on security intelligence and emerging technologies.	KE1: Emerging developments in cyber security technologies and threat intelligence, methods for implementing threat management systems, ethical and proportionate application of security technologies, and associated legislative and regulatory frameworks.
2. Data security and privacy	K5: Emerging developments in data security solutions. K6: Methods for implementing data security approaches. K7: Legislative and regulatory frameworks relating to data protection and privacy.	S3: Analyse developments in data security, privacy governance and regulatory compliance, applying this analysis to complex workplace practice. S4: Design and apply data security frameworks incorporating privacy	PE2: Resolve a complex data security or privacy compliance issue by developing and applying data security frameworks incorporating governance and compliance mechanisms.	KE2: Emerging developments in data security solutions, methods for implementing data security approaches, and associated legislative and regulatory frameworks for data protection and privacy.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
		governance and compliance mechanisms.		
3. Incident response and communication	K8: Methods for implementing incident response frameworks.	S5: Take responsibility for the quality of incident response practice within a team or work area, including communication protocols and recovery approaches. S6: Contribute specialist expertise to improving incident response maturity and resilience.	PE3: Take responsibility for the quality of incident response practice within a team or work area, including communication protocols and recovery approaches, and contribute to improving incident response maturity and resilience.	KE3: Methods for implementing incident response frameworks in workplace contexts.
4. Security culture and policy	K9: Approaches for building cyber security capability in others.	S7: Assess security culture models, governance frameworks and capability-building approaches, applying this analysis to complex workplace situations. S8: Apply and contribute to security culture and governance frameworks that embed accountability. S9: Provide expert advice and mentoring to build another person's advanced capability in cyber security practice.	PE4: Evaluate security culture models, governance frameworks or capability-building approaches as they apply to a complex workplace situation and provide expert advice or mentoring to build another person's cyber security capability.	KE4: Approaches for building organisational cyber security capability and culture.

DRAFT

BSBDIG508X — Develop Highly Advanced Digital Skills in the Workplace

This UoCs Performance Evidence is deliberately structured as broad, cross-domain statements reflecting the UoCs integration purpose at the highest level; several items span most or all of the unit's five digital capability areas rather than one or two. Full text is shown against the area listed first in the UoC; other areas evidenced are noted, with a short cross-reference shown in those areas' Performance Evidence column.

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
1. Information search, evaluation and management	K1: Emerging trends across digital search technologies and methodologies. K2: Frameworks for information validation and governance. K3: Approaches to information resilience.	S1: Synthesise developments in digital search technologies and information management systems to inform workplace decisions. S2: Take responsibility for the quality of search and evaluation work within a team or work area, integrating advanced strategies with systematic evaluation approaches. S3: Manage comprehensive data and information practices that contribute to organisational governance. S4: Contribute specialist expertise to strengthening organisational resilience to misinformation and disinformation.	PE1: Combine digital capabilities across information management, communication, content creation and problem-solving to resolve a complex, cross-domain workplace challenge (also evidences Area 2, Communication and collaboration; Area 3, Digital content creation; and Area 5, Problem identification and solving). PE2: Evaluate developments across all digital capability areas, including search technologies, communication platforms, content tools and cyber security requirements, to inform a workplace decision (also evidences Area 2, Communication and collaboration; Area 3, Digital content creation; and Area 4, Safety, wellbeing and responsible use).	KE1: Emerging trends across digital search technologies and methodologies, frameworks for validating and governing information, and approaches for building resilience to unreliable information.
2. Communication and collaboration	K4: Emerging trends across communication and collaboration platforms. K5: Frameworks for	S5: Combine and optimise communication technologies for complex tasks spanning multiple	PE1: (see Area 1 above — Combine digital capabilities across information management,	KE2: Emerging trends across communication and collaboration platforms, frameworks for

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
	communication approaches. K6: Ethical and proportionate use of AI in communication and collaboration. K7: Legislative and regulatory frameworks relating to digital behaviour.	stakeholders or platforms. S6: Facilitate collaborative approaches that enable ethical AI use and effective human-AI collaboration. S7: Analyse the societal, economic and political impacts of digital technologies, applying this analysis to workplace decisions involving digital behaviour and rights.	communication, content creation and problem-solving). PE2: (see Area 1 above — Evaluate developments across all digital capability areas). PE5: (see Area 5 below — Build organisational capability by mentoring others, developing learning resources and promoting ethical and inclusive practice).	communication approaches, the principles of ethical and proportionate AI use in collaboration, and legislative and regulatory frameworks relating to digital behaviour.
3. Digital content creation	K8: Emerging trends across content creation technologies. K9: Frameworks for content quality management and intellectual property. K10: Legislative and regulatory frameworks relating to copyright.	S8: Produce content for complex or unfamiliar purposes using advanced design, data visualisation and integration techniques, embedding accessibility, inclusivity and ethical practice. S9: Address complex copyright or licensing questions by applying intellectual property knowledge. S10: Integrate automation or AI systems within complex workplace processes, drawing on specialist knowledge.	PE1: (see Area 1 above — Combine digital capabilities across information management, communication, content creation and problem-solving). PE2: (see Area 1 above — Evaluate developments across all digital capability areas). PE4: Apply advanced design, data visualisation and content integration techniques to a complex challenge, while taking responsibility for related organisational approaches to cyber security, data protection or device security (also evidences Area 4, Safety, wellbeing and responsible use).	KE3: Emerging trends across content creation technologies, frameworks for content quality management and intellectual property, and legislative and regulatory frameworks relating to copyright.
4. Safety,	K11: Emerging trends across	S11: Resolve complex cyber	PE2: (see Area 1 above —	KE4: Emerging trends

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
wellbeing and responsible use	cyber security and privacy solutions and sustainability impacts. K12: Frameworks for safety and wellbeing evaluation. K13: Approaches to accessibility and inclusion, data protection and sustainability. K14: Legislative and regulatory frameworks relating to cyber security, data protection, wellbeing, inclusion, and environmental sustainability.	security or data protection compliance questions by interpreting relevant legislation and take responsibility for the quality of related protective practices within a team or work area. S12: Evaluate evidence relating to wellbeing and inclusion in digital environments, embedding safe, inclusive and equitable digital practices. S13: Draw on specialist knowledge of environmental impacts to promote sustainable digital practices.	Evaluate developments across all digital capability areas). PE4: (see Area 3 above — Apply advanced design, data visualisation and content integration techniques to a complex challenge).	across cyber security, privacy and sustainability considerations, frameworks for evaluating safety and wellbeing, approaches to accessibility, inclusion, data protection and sustainability, and associated legislative and regulatory frameworks.
5. Problem identification and solving	K15: Emerging trends across problem-solving methodologies. K16: Frameworks for capability development. K17: Methods for developing integrated solutions, implementing change, contributing to organisational standards and building capability in others.	S14: Design and deliver training that builds confidence and autonomy in others to resolve technical or user-need problems using digital technologies. S15: Provide expert mentoring and develop learning resources to build another person's digital competence.	PE1: (see Area 1 above — Combine digital capabilities across information management, communication, content creation and problem-solving). PE3: Contribute to an integration initiative spanning multiple digital capability areas, applying digital technologies to a complex problem-solving scenario (this item explicitly spans multiple digital capability areas of this unit). PE5: Build organisational capability by mentoring others, developing learning	KE5: Emerging trends across problem-solving methodologies, frameworks for capability development, and methods for developing integrated solutions, implementing change, contributing to organisational standards and building capability in others.

DRAFT

Digital Capability Area	Knowledge	Skills	Performance Evidence	Knowledge Evidence
			resources and promoting ethical and inclusive practice, including supporting others to understand their digital behaviour rights and responsibilities (also evidences Area 2, Communication and collaboration).	

DRAFT

Section 2 – Recognition of Prior Learning Guidance

2.1 Overview

The Digital Capability UoCs support Recognition of Prior Learning (RPL) and assessment-only pathways across all digital capability areas and proficiency levels. Significant digital capability is acquired through work, community participation, previous study, self-directed learning and life experience, much of which may not be formally recognised. This section provides guidance to support RTOs to design and conduct rigorous, fair and efficient RPL processes for all 32 UoCs.

This section provides RPL guidance organised by digital capability area, with each sub-section covering all four proficiency levels. The guidance supports:

- identifying suitable RPL candidates
- determining the appropriate proficiency level for assessment
- designing evidence portfolios that demonstrate digital capability
- conducting assessment interviews and observations to verify digital capability
- making inference judgements where direct evidence is limited
- priority cohort guidance.

This guidance also supports RTOs in developing assessment tools and structured professional conversations. The evidence examples can inform the design of portfolio assessment tasks and workplace observation checklists. The assessor prompts are suitable for use in assessment interviews and professional conversations, not only RPL contexts.

2.2 Quick-reference digital capability matrix

The matrix below summarises the digital capability expected at each proficiency level across all seven digital capability areas. Use this matrix to navigate to the detailed guidance in Section 5.2, and to support initial conversations with RPL candidates about their level of digital capability.

Digital Capability Area	Basic	Intermediate	Advanced	Highly Advanced
1. Info Search, Eval & Management	Follow procedures to locate, check and organise workplace information.	Conduct targeted searches; evaluate sources; manage files across systems.	Combine tools strategically; govern information; support others.	Lead information management digital capability; apply governance frameworks.
2. Communication & Collaboration	Use digital tools for communication and collaboration following workplace procedures.	Select tools purposefully; engage ethically; manage digital identity.	Coordinate complex collaboration; advise others; manage multi-platform identity.	Lead communication digital capability; govern digital behaviour and identity.
3. Digital Content Creation	Create and edit content using templates; follow copyright basics; use basic automation features.	Create across formats; apply AI ethically; use Intellectual Property (IP) principles.	Produce complex content; assess AI ethics; apply computational thinking.	Lead content strategy; govern IP and automation; build digital capability.

DRAFT

Digital Capability Area	Basic	Intermediate	Advanced	Highly Advanced
4. Safety, Wellbeing & Responsible Use	Follow device protection and privacy procedures; support wellbeing; apply environmentally responsible practices.	Manage privacy across contexts; review wellbeing; apply sustainability.	Guide others in cyber security and privacy; support wellbeing; evaluate environmental impact.	Lead safety and sustainability governance; build organisational digital capability.
5. Problem Identification & Solving	Troubleshoot common issues; use digital assistance tools.	Troubleshoot varied problems; assess accessibility; support others digital capability development.	Apply advanced problem-solving; assess technologies; coach others.	Lead complex problem-solving; mentor others; direct digital capability development.
6. AI	Complete routine tasks using AI tools with verification and disclosure.	Use multiple AI tools; evaluate outputs; manage AI risks; integrate AI into workflows.	Implement AI solutions; challenge outputs; apply responsible AI; coach others.	Lead AI integration; govern AI risk; apply human-centred practice; build digital capability.
7. Cyber Security	Recognise threats; follow security protocols; report incidents.	Respond to threats; apply access controls; contribute to security culture.	Assess threats; implement security; coordinate incident response; develop security culture.	Lead threat management; govern data security; lead incident response; direct security culture.

DRAFT

2.2 RPL Guidance by Digital Capability Area

The following sub-sections provide detailed RPL guidance for each of the seven areas, covering all four proficiency levels. Each sub-section includes a proficiency-level table showing typical candidate profiles, evidence examples and assessment approaches at each level.

This information is provided as guidance only and RTOs remain responsible for ensuring requirements for each UoC are met.

2.2.1 Information Search, Evaluation and Management

This digital capability area is about finding, evaluating, organising and managing digital information and data. It underpins evidence-based workplace decision-making and information governance across all industries.

RPL candidates will typically have developed capability through:

- workplace research and information-gathering tasks
- file and records management responsibilities
- source evaluation in roles requiring evidence-based decision-making
- data management and reporting duties
- personal digital practices including online research and file organisation.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG201X	Candidate: • locates and accesses relevant information by following workplace procedures • applies workplace fact-checking and verification steps to confirm credibility relevance • organises, stores and retrieves digital files using workplace templates and systems.	• Screenshots of search queries used to locate workplace information, with results saved or shared. • Examples of applying a workplace fact-checking procedure before using or sharing information. • Organised folder or file structures created using workplace naming conventions and templates. • Supervisor or third-party confirmation that routine information search and filing tasks were completed correctly.	"*Walk me through how you would find a specific piece of information using the tools available to you at work."* *"Tell me about a time you needed to check whether information was accurate before using it. What steps did you take?"* *"Describe how you organise your digital files at work.* *What system do you use and how did you learn it?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
Intermediate BSBDIG301X	Candidate: • conducts targeted searches using appropriate tools, advanced functions and filters across varied workplace contexts • evaluates credibility and reliability by identifying sources, applying fact-checking techniques, recognising bias and misinformation, and assessing AI-generated content • organises and manages digital information using consistent naming conventions, folder structures and multiple storage locations, and uses data collection tools • applies basic formulas to process data in structured digital environments • works with limited supervision.	• Research completed for a workplace project showing tool selection, search strategies and source evaluation • Documented fact-checking or credibility assessment applied before acting on or sharing information • Examples of identifying bias, misinformation or unreliable AI-generated content in a work context • File management systems using consistent naming conventions across multiple storage locations • Examples of using data collection tools and applying basic formulas to process data in a structured digital environment • Evidence of applying ethical data handling procedures within a workplace context	*"Walk me through how you would evaluate whether a source is credible enough to use for a workplace task."* *"Describe a time you came across AI-generated content at work. How did you assess whether it was accurate?"* *"How do you decide which search tool or platform to use for different types of information tasks?"* *"Tell me about a time you used a data collection tool or applied formulas to process workplace data. What was the task and how did you set it up?"*
Advanced BSBDIG401X	Candidate: • evaluates and selects advanced search tool features including vendor and tool assurance considerations; combines multiple tools and strategies to address complex information requirements; analyses how AI systems, bias, vested interests and algorithmic curation influence digital information; • applies multiple validation methods; • implements governance-compliant information management practices;	• Strategic research or information-gathering projects combining multiple tools and sources • Documented analysis of AI bias, misinformation, algorithmic influence or manipulated content • Information governance frameworks, data protection protocols or security procedures developed or implemented • Complex analytical reports drawing on evaluated data from multiple sources to support decision-making	*"Tell me about the most complex information-gathering task you have led. How did you select and validate your sources?"* *"Describe how you have analysed the influence of AI systems or algorithmic content on information your organisation uses."* *"How have you supported colleagues to improve their digital search, evaluation or information management practices?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	analyses complex information to support workplace decision-making; • supports and guides others to develop digital search, evaluation and management capability.	• Training materials, guidance notes or mentoring records showing support provided to colleagues • Evidence of applying open data or big data sources within a workplace information task	
Highly Advanced BSBDIG501X	Candidate: • assesses and evaluates emerging developments in digital search and information management technologies to support organisational decision-making • leads complex information initiatives integrating multiple tools and strategies; promotes organisational resilience to misinformation and disinformation • develops and applies governance frameworks for complex data and information management including big data techniques • leads workplace capability-building initiatives • contributes to improvements in complex information challenges across search, evaluation and management.	• Evaluations of emerging search or information management technologies informing organisational strategy • Misinformation or disinformation resilience initiatives designed and led at team or organisational level • Governance frameworks or structured data management approaches developed and applied across an organisation • Complex information management initiatives using big data tools, methods or platforms • Capability-building programs or professional development led for others in digital information competencies • Documented contributions to improvements in organisational information challenges spanning search, evaluation and management	*"How have you evaluated emerging information or search technologies and used that assessment to influence organisational direction?"* *"Describe an initiative you have led to build your organisation's resilience to misinformation or disinformation."* *"Tell me about a governance framework or structured data management approach you have developed. What drove the design decisions?"*

DRAFT

2.2.2 Communication and Collaboration

This digital capability area is about using digital tools to communicate, collaborate and participate in workplace and online environments. It includes digital behaviour, digital identity management and ethical engagement in digital spaces.

RPL candidates will typically have developed capability through:

- workplace digital communication: email, messaging platforms, video conferencing
- collaborative work in shared digital spaces (Teams, SharePoint, Google Workspace)
- managing professional digital presence and identity
- community participation in digital environments
- coordination of digital events or communications across teams.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG202X	Candidate • communicates using digital tools and platforms both synchronously and asynchronously • shares information and content securely through appropriate digital channels • participates in workplace or community activities and collaborative groups using workplace-approved digital platforms • demonstrates appropriate digital behaviour and manages their digital identity.	• Examples of digital messages, emails or posts sent through workplace-approved channels showing appropriate tone and format • Records of participation in a digital meeting, group chat or online collaboration platform • Evidence of following workplace procedures for secure information sharing, including what can and cannot be shared • Supervisor confirmation of appropriate online behaviour maintained in workplace digital environments • Examples of managing digital identity such as maintaining a professional profile or following access controls	*"Describe how you communicate with colleagues or clients using digital tools at work. What platforms do you use and how do you decide what to send where?"* *"Tell me about a time you needed to share information digitally. How did you make sure it was sent securely and to the appropriate people?"* *"How do you manage your digital identity at work? What steps do you take to protect your information online?"*
Intermediate BSBDIG302X	Candidate: • selects appropriate digital communication tools based on context and purpose	• AI prompts developed for workplace interactions, including records of disclosure or attribution of AI-generated content	*"Tell me about the time you used an AI system in a communication or collaboration task. How did you handle disclosure or attribution of AI-*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	• develops prompts for AI system interactions including disclosure and attribution of AI-generated content • shares information effectively and ethically across varied digital environments including assessing risks and benefits; • reports misinformation and ensures appropriate attribution and security; participates in a workplace or community activity using digital platforms and services, weighing up the risks and benefits of their use • coordinates and contributes to collaborative tasks with ethical human-AI collaboration; demonstrates respectful digital behaviour across formal and informal contexts and diverse audiences • manages digital identity across multiple platforms.	• Evidence of assessing risks and benefits before sharing information across digital environments • Examples of reporting misinformation or ensuring correct attribution and security of shared content • Records of participating in a workplace or community activity using digital platforms or services, with risks and benefits considered • Records of coordinating or contributing to collaborative digital tasks, including ethical human-AI collaboration • Evidence of managing digital identity across multiple platforms including adjusting settings and maintaining professional presence	*generated content?"* *"Describe how you manage your digital identity across the platforms you use at work. What do you check or adjust and why?"* *"Tell me about a workplace or community activity you've taken part in using digital platforms. What risks or benefits did you consider?"*
Advanced BSBDIG402X	Candidate: • selects and combines digital communication tools for complex workplace tasks • develops and refines AI prompts for complex interactions • coordinates or facilitates complex digital events and assists others with tool selection; shares information ethically and advises others on ethical sharing practices • assesses digital technologies for inclusion, exclusion and democratic impacts	• Complex communication plans or multi-tool communication projects developed and implemented • AI prompt development and refinement for complex workplace interactions, with documented iterations and outcomes • Records of facilitating or coordinating complex digital events, including guiding others on tool use	*"Describe a complex communication task you have managed using multiple digital tools. How did you decide which tools to use and how did you support others?"* *"Tell me about a time you developed or refined prompts for an AI system in a workplace context. What did you learn through that process?"* *"How have you assessed a digital technology or AI tool?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	including high-risk AI systems; responds to challenging digital situations while promoting inclusive behaviour; implements digital identity management.	• Documented ethical assessment of a digital technology or AI system including analysis of inclusion or democratic impacts	
Highly Advanced BSBDIG502X	Candidate: • assesses and combines communication tools for complex tasks and leads improvements in tool use across the organisation • leads complex information sharing initiatives across varied technologies; evaluates digital technology impacts on society, political processes and the economy; leads digital citizenship initiatives • promotes ethical and proportionate AI use and leads improvements in human-AI collaboration • supports others to understand rights and responsibilities under digital behaviour legislation; advises on complex identity management • critically evaluates emerging developments to inform and adapt own highly advanced practice.	• Organisational communication tool evaluations or improvement initiatives designed and led • Complex information sharing strategies or cross-technology communication approaches developed and applied • Analysis or reports evaluating the societal, political or economic impacts of digital technologies • Digital citizenship initiatives led at team or organisational level including policy implementation or behaviour change programs • Evidence of promoting ethical and proportionate AI use in communication or collaboration contexts • Guidance or advisory work supporting others on digital behaviour legislation, identity management rights or complex identity challenges • Critical evaluations of emerging communication or collaboration technologies informing strategic practice	*"How have you led improvements in how your organisation uses digital communication tools? What drove the changes and how did you implement them?"* *"Describe an initiative you have led around digital citizenship or ethical technology use. What was your specific contribution and what was the outcome?"* *"Tell me how you have evaluated emerging communication or collaboration technologies and used that to adapt your own practice or advise others."*

DRAFT

2.2.3 Digital Content Creation

This digital capability area is about creating, editing and adapting digital content across formats and tools. It includes content development, integration and adaptation, copyright and licensing, and computational thinking and programming.

RPL candidates will typically have developed capability through:

- workplace content creation: images, video, infographics, social media content
- template-based content development and editing
- applying copyright and licensing requirements in content creation roles
- using automation tools and AI systems in content workflows.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG203X	Candidate: • creates and edits digital content using workplace tools and templates • modifies and integrates existing content in line with workplace formatting and quality guidelines; applies copyright, licensing and ethical guidelines when creating and sharing content • uses basic automation features to support routine content creation tasks.	• Digital content created or edited using workplace tools and templates, such as documents, presentations or social posts • Examples of modifying or integrating existing content to meet workplace formatting or quality requirements • Evidence of applying copyright or licensing procedures before using or sharing digital content • Examples of using basic automation features in a workplace tool to support a routine content task • Supervisor confirmation that AI-generated content was checked for accuracy and appropriateness before use	*"Show me an example of digital content you have created or edited at work. Walk me through how you used the tools and followed your workplace guidelines."* *"Tell me about a time you used or adapted existing content for a workplace task. How did you make sure you were allowed to use it?"* *"Have you used any automation or AI features to help with content creation at work? How did you check the output was suitable?"*
Intermediate BSBDIG303X	Candidate • creates and edits digital content across multiple formats using a range of tools, identifying and addressing audience and accessibility needs	• Digital content created across multiple formats — for example documents, graphics, video or data visualisations — with audience and accessibility needs addressed	*"Describe a content creation task where you had to consider the audience and accessibility requirements. How did you approach it?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	• modifies, integrates and transforms existing content to meet specific requirements using AI systems ethically and transparently with appropriate disclosure and attribution • applies copyright, licensing and intellectual property principles • applies computational thinking to routine processes including creating visual representations and identifying automation opportunities.	• Examples of transforming or adapting existing content to meet specific format, structure or audience requirements • Records of using AI systems for content creation with appropriate disclosure and attribution documented • Evidence of applying copyright, trademark or licensing principles when using or sharing content in a workplace context • Visual representations of workplace processes or basic algorithms developed using computational thinking • Examples of identifying and applying automation tools to support routine workplace content tasks	*"Tell me about a time you used an AI system to help create or transform content. How did you handle disclosure and attribution?"* *"Have you mapped out a workplace process or created a basic algorithm? Walk me through how you approached that task."*
Advanced BSBDIG403X	Candidate • selects and combines content creation tools and methods to produce accessible complex or specialised digital content; integrates and adapts diverse content to meet complex format, structure and audience requirements • assesses ethical and practical considerations for AI systems and automation • applies copyright, licensing and intellectual property guidelines in complex contexts; applies computational thinking and uses automation tools • systematically evaluates content against quality, accessibility and usability criteria	• Complex or specialised digital content produced by combining multiple tools and methods, with accessibility addressed • Documented ethical assessments of AI systems or automation tools used in content creation or integration tasks • Evidence of applying copyright and intellectual property guidelines in complex content contexts, including AI training data considerations • Automation scripts, workflows or AI system configurations developed to automate routine content tasks	*"Describe a complex content creation project you have led. How did you select and combine tools, and how did you ensure accessibility and quality?"* *"Tell me about a time you assessed whether an AI system or automation tool was appropriate for a content task. What ethical or practical considerations did you apply?"* *"How have you supported others to develop their digital content creation or computational thinking capability?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	and refines based on feedback; supports others to develop capability in ethical content creation.	• Systematic content evaluations against quality, accessibility and usability criteria with refinements documented • Training materials, guidance or mentoring records showing capability development supported in others	
Highly Advanced BSBDIG503X	Candidate: • leads complex content creation and integration initiatives applying advanced design and data visualisation techniques • develops and applies improvements for complex content challenges; promotes accessibility, inclusivity, ethical and transparent practices across content initiatives; contributes to workplace frameworks and standards for content creation • leads implementation of copyright and licensing policies; leads complex automation or AI system projects; builds organisational capability in content creation and automation • monitors emerging developments in content technologies to inform workplace practice.	• Complex content creation or integration initiatives led, applying advanced design or data visualisation techniques • Workplace frameworks, standards or guidelines for content creation contributed to or developed • Copyright or licensing policies implemented, or improvements led at an organisational level • Complex automation or AI system projects led, with ethical use promoted throughout • Capability-building programs or professional development led for others in content creation, integration or automation • Documented monitoring of emerging content technologies, copyright requirements or AI developments informing workplace practice	*"Describe a complex content creation or integration initiative you have led. How did you apply advanced design or data visualisation techniques to address the challenge?"* *"Tell me about a framework or standard for content creation you have contributed to or led. What drove the design decisions and how was it implemented?"* *"How have you monitored emerging developments in content technologies or AI to inform your organisation's practice? What actions resulted?"*

DRAFT

2.2.4 Digital Safety, Wellbeing and Responsible Use

This digital capability area is about protecting devices, personal data, privacy, health, wellbeing and the environment in digital contexts. It includes device protection, personal data and privacy management, digital wellbeing and environmental sustainability.

RPL candidates will typically have developed capability through:

- workplace cyber security and privacy practices
- personal device and account management including strong passwords and multi-factor authentication
- workplace wellbeing programs with digital components
- environmental and sustainability practices in digital tool use
- roles with data handling, privacy compliance or incident reporting responsibilities.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG204X	Candidate: • follows workplace procedures for device protection including strong passwords and multi-factor authentication • follows workplace procedures for personal data security; applies workplace wellbeing guidelines to support personal digital habits • follows environmentally responsible practices when using digital technologies.	• Evidence of following workplace password and multi-factor authentication procedures, such as a completed security setup or supervisor confirmation • Examples of applying personal data security procedures in a workplace context, including what information was protected and how • Records of following workplace wellbeing guidelines related to digital use, such as screen time practices or break schedules • Examples of applying environmentally responsible digital practices, such as device power management or responsible disposal procedures • Position description or workplace induction records confirming responsibilities for digital security and responsible use	*"Walk me through the security measures you use for your devices at work. What procedures do you follow and why?"* *"Tell me about how you protect your personal data at work. What steps do you take and what does your workplace require?"* *"How do you manage your digital wellbeing at work? What practices do you follow to support your health when using technology?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
Intermediate BSBDIG304X	Candidate: • applies prevention techniques to protect devices and content in accordance with workplace procedures, including recognising AI systems used in cyber attacks • manages personal data and privacy across varied digital environments using privacy tools • reviews and adapts digital usage patterns to support physical, mental and social wellbeing; responds to harmful behaviour and content • implements environmental sustainability strategies across the full device lifecycle including AI system impacts.	• Examples of applying device protection techniques in response to identified threats, including AI-assisted cyber-attack recognition • Evidence of managing personal data and privacy across varied digital environments using privacy tools, including data removal or anonymisation • Records of reviewing and adapting digital usage patterns to address wellbeing concerns — physical, mental or social • Examples of identifying and responding to harmful digital content or behaviour, including bias amplification or exclusion • Evidence of applying environmental sustainability strategies across device purchasing, usage, repair or disposal decisions	*"Describe how you protect your devices and content from cyber threats at work. Have you encountered or recognised an AI-assisted attack? How did you respond?"* *"Tell me about how you manage your privacy across the digital platforms you use. What tools or strategies do you apply?"* *"How do you consider environmental sustainability when making decisions about digital technology — purchasing, using or disposing of devices?"*
Advanced BSBDIG404X	Candidate: • updates and prioritises cyber security measures in response to evolving threats • guides and supports others to implement device protection; supports others to understand rights and obligations under data protection and privacy legislation • coaches individuals and teams on personal data protection strategies; facilitates wellbeing reviews and adaptations with individuals and teams • identifies and responds to harmful behaviour, content and deceptive design • builds capacity of others to counter digital bias and exclusion	• Evidence of updating or reprioritising cyber security measures in response to evolving or emerging threats • Records of guiding or training others to implement device protection measures or understand their rights under privacy legislation • Coaching or support provided to individuals or teams on personal data protection and privacy management strategies • Facilitated wellbeing reviews or digital usage adaptation sessions conducted with individuals or teams	*"Describe a time you updated or reprioritised cyber security measures in response to an evolving threat. What drove the decision and how did you implement it?"* *"Tell me about how you have supported others to understand their rights or implement strategies under data protection or privacy legislation."* *"How have you helped individuals or teams review and adapt their digital technology use to support wellbeing or reduce environmental impact?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	• evaluates environmental impacts and advises others on reducing impact.	• Examples of identifying deceptive design, harmful content or digital bias and responding or building others' capacity to respond • Environmental impact evaluations of digital technologies with recommendations provided to others	
Highly Advanced BSBDIG504X	Candidate: • assesses and interprets cyber security legislation and leads citizen-focused cyber security initiatives • applies data protection and privacy policy requirements to inform organisational decision-making and leads implementation of data protection strategies; promotes responsible and ethical digital practices including risk and accountability • evaluates wellbeing and inclusion evidence and leads initiatives embedding wellbeing into digital systems • contributes to organisational decision-making about digital change • leads digital sustainability initiatives; mentors others • monitors and critically evaluates emerging developments to inform strategic decision-making.	• Assessments or interpretations of cyber security legislation informing organisational strategy or citizen-focused initiatives led • Data protection strategies developed and led at an organisational level, drawing on policy and legislative requirements • Wellbeing and inclusion initiatives designed and led that embed wellbeing considerations into digital systems or workplace practices • Contributions to organisational decision-making about digital change, including risk and accountability considerations documented • Digital sustainability programs or improvement initiatives led at team or organisational level • Mentoring records or capability-building programs led for others in cyber security, data protection or responsible digital use • Critical evaluations of emerging developments in cyber security, privacy or sustainability informing strategic workplace decisions	*"How have you interpreted or applied cyber security legislation to lead an initiative in your workplace? What was your specific contribution and what was the outcome?"* *"Describe an initiative you have led to embed digital wellbeing or inclusion into your organisation's systems or practices. How did you evaluate its effectiveness?"* *"Tell me how you monitor emerging developments in cyber security, data protection or digital sustainability and use that to inform strategic decisions at work."*

DRAFT

2.2.5 Digital Problem Identification and Solving

This digital capability area is about identifying needs and resolving problems through appropriate digital tools and approaches. It includes solving technical problems, identifying needs and digital technological responses, applying creative digital solutions, and addressing digital capability gaps.

RPL candidates will typically have developed capability through:

- workplace troubleshooting and technical problem-solving
- identifying digital tool needs and selecting or recommending solutions
- supporting colleagues with digital access, accessibility or technical issues
- self-directed digital learning and capability development
- community digital support roles: volunteering, peer support, community organisations.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG205X	Candidate: • identifies and resolves common technical problems following workplace procedures; follows established procedures to update software and applications • uses digital assistance tools and assistive technologies for simple workplace tasks • adjusts digital environment settings to meet a specified user need; reviews own digital capability • can describe how digital technologies support problem-solving or creativity using workplace examples.	• Examples of identifying and resolving a common technical problem at work, with steps taken documented • Records of following workplace procedures to update software or applications on a device • Evidence of using a digital assistance tool or assistive technology to support a routine workplace task • Screenshots or records showing digital environment settings adjusted to meet a user need or preference • A self-assessment or reflection identifying a digital capability gap and a specific source of support or learning identified • Supervisor confirmation that digital problem-solving procedures were followed correctly	*"Tell me about a technical problem you have encountered at work. Walk me through how you identified it and what steps you took to resolve it."* *"Describe how you keep your software or devices up to date at work. What procedures do you follow?"* *"Where do you feel your digital skills could be stronger? What would you do to build that digital capability?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
Intermediate BSBDIG305X	Candidate • troubleshoots technical problems using varied human-assisted and technology-assisted strategies • updates and adjusts device settings to maintain performance and meet workplace requirements; adjusts digital environment features and uses digital assistance tools to support diverse needs • identifies strengths and limitations of digital technologies for specific problem-solving tasks and uses them responsibly and ethically • reviews own digital capability and identifies relevant learning opportunities.	• Examples of troubleshooting technical problems using a combination of human-assisted and technology-assisted strategies, with reasoning documented • Records of adjusting device settings or digital environment features to maintain performance or support diverse user needs • Evidence of assessing whether a digital technology is appropriate for a specific problem-solving task, including ethical considerations • Examples of using digital technologies responsibly and ethically to solve problems individually or as part of a team • A documented review of own digital capability identifying specific learning opportunities pursued or planned	*"Describe a technical problem you have troubleshot at work. What strategies did you use and how did you decide between human-assisted and technology-assisted approaches?"* *"Tell me about a time you assessed whether a digital technology was the right tool for a problem-solving task. What strengths or limitations did you identify?"* *"How do you keep your digital skills current? What learning opportunities have you identified and pursued recently?"*
Advanced BSBDIG405X	Candidate: • troubleshoots technical problems using varied solution-finding strategies and supports others to diagnose and resolve problems • adjusts digital environment features to meet diverse needs and assesses accessibility, inclusivity and fairness • supports others to make informed use of digital assistance tools; applies digital technologies efficiently, responsibly and ethically to solve problems including non-routine challenges; contributes to digital problem-solving initiatives;	• Records of troubleshooting complex or non-routine technical problems using advanced • solution-finding strategies, with approach documented • Examples of supporting others to diagnose and resolve technical problems, including guidance or coaching provided • Assessments of digital technology accessibility, inclusivity, fairness or rights-sensitivity conducted and acted upon • Evidence of contributing to an initiative applying digital technologies to a workplace problem-solving challenge	*"Describe the most complex technical problem you have resolved. What solution- finding strategies did you apply and how did you support others through the process?"* *"Tell me about a time you assessed a digital technology for accessibility, inclusivity or fairness. What did you find and what action did you take?"* *"How have you coached or supported others to build their digital problem-solving capability or confidence?* *What approaches have you used?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	• assesses digital technological developments • guides and supports others to develop digital capability, confidence and autonomy.	• Coaching or mentoring records showing digital capability, confidence or autonomy developed in others • Documented review of digital technological developments and implications for own or team digital capability	
Highly Advanced BSBDIG505X	Candidate: • promotes inclusive and accessible digital technologies and contributes to improvements in digital assistance tools • assesses complex needs and tailors digital solutions; leads initiatives applying digital technologies to complex problem-solving • monitors personal development needs and engages in ongoing self-development • mentors others to build confidence, autonomy and capability in technical problem-solving and to identify and address their individual digital	• Contributions to improvements in digital assistance tools or accessible technology evaluations at team or organisational level • Complex needs assessments conducted with tailored digital solutions developed and implemented • Digital problem-solving initiatives led in workplace contexts applying digital technologies to complex challenges • Mentoring records showing others supported to build technical problem-solving confidence, autonomy and digital capability • Training programs, learning resources or capability-building materials developed or delivered for complex digital capability • Personal development records demonstrating ongoing self-assessment and targeted digital skill development	*"Describe an initiative you have led that applied digital technologies to a complex problem-solving challenge in your workplace. What was your approach and what was the outcome?"* *"Tell me about how you have mentored others in technical problem-solving or digital capability development. How did you tailor your approach to individual needs?"* *"Describe training or learning resources you have developed or delivered for complex digital capability. How did you design them and how did you evaluate their effectiveness?"*

DRAFT

2.2.6 AI

This digital capability area is about understanding, using and critically evaluating AI systems in workplace contexts. It spans basic AI awareness through to strategic AI leadership, reflecting the DEC AI Literacy Framework and Australian Government AI governance guidance.

RPL candidates will typically have developed capability through:

- workplace AI tool use: for example: Microsoft 365 Copilot, ChatGPT, sector-specific AI tools
- developing AI prompts and evaluating AI outputs in workplace tasks
- applying workplace AI disclosure and attribution requirements
- contributing to workplace AI governance or policy
- self-directed learning about AI capabilities, limitations and risks
- leading AI implementation or integration initiatives.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG206X	Candidate: • completes a routine workplace task using an approved AI tool, verifies the AI-generated output against another source, and records or discloses the AI contribution in line with workplace requirements • handles data and sensitive information safely and lawfully when using AI tools; follows workplace incident response and escalation procedures when an AI output is unclear, • inappropriate, harmful or requires human oversight.	• Examples of a routine task completed using an approved workplace AI tool, with verification against another source documented • Records of disclosing or attributing AI contributions in line with workplace requirements • Evidence of following workplace privacy and safety procedures when handling data or sensitive information with AI tools • Records of escalating or responding to an AI output that was unclear, inappropriate or required human oversight, following workplace procedures • Supervisor confirmation that AI tool use, verification and disclosure procedures were followed correctly	*"Tell me about a routine task you have completed using an AI tool at work. How did you verify the output and how did you record or disclose the AI contribution?"* *"Describe how you handle data or sensitive information when using AI tools. What workplace procedures do you follow?"* *"Have you ever received an AI output that seemed unclear, wrong or inappropriate? What did you do?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
Intermediate BSBDIG306X	Candidate: • uses at least two different AI tools systematically to complete routine workplace tasks; evaluates AI outputs, identifies limitations, bias and synthetic or manipulated content, and applies verification procedures • implements AI risk management protocols covering privacy, data security, lawful data handling, incident response and escalation • coordinates human judgement with AI capabilities including transitions and quality controls integrates AI tools into workplace procedures with appropriate disclosure and attribution.	• Examples of using at least two different AI tools systematically for workplace tasks, with tool selection reasoning documented • Documented evaluations of AI outputs identifying limitations, bias or synthetic and manipulated content, with verification applied • Records of implementing AI risk management protocols — privacy protection, lawful data handling, incident response or escalation • Evidence of coordinating human judgement with AI capabilities, including quality control measures applied at human-AI transitions • Examples of integrating AI tools into workplace procedures with disclosure and attribution of AI-generated content documented	*"Walk me through how you select and use different AI tools for workplace tasks. How do you evaluate which tool is appropriate and how do you verify the outputs?"* *"Describe how you manage AI-related risks at work — privacy, data handling, incident response. Give me a specific example."* *"Tell me about a time you needed to apply human judgement to an AI output before acting on it. How did you make that decision?"*
Advanced BSBDIG406X	Candidate: • uses at least three different AI tools to implement AI-enabled solutions across workplace processes • demonstrates AI applications and shares structured approaches to promote practical AI use among others • evaluates AI outputs and system performance using professional judgement and defined quality criteria; identifies limitations, bias, inconsistency and error in AI-generated results • applies ethical AI principles, data governance and privacy controls; manages AI-related risks; embeds appropriate human oversight and	• AI-enabled solutions implemented across workplace processes using at least three different AI tools, with approach documented • Structured demonstrations or guidance materials developed to promote practical AI use among colleagues • Systematic evaluations of AI outputs and system performance against defined quality criteria, with limitations and bias identified • Records of applying ethical AI principles, data governance requirements and privacy controls in AI implementation • AI risk management records including incident identification and response actions taken	*"Describe an AI-enabled solution you have implemented across a workplace process. How did you select the tools, evaluate outputs and manage the associated risks?"* *"Tell me about how you have supported or guided others to use AI tools responsibly and effectively. What approach did you take?"* *"How have you applied ethical AI principles or data governance requirements in a real workplace context? What decisions did that shape?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	verification supports and guides others to use AI responsibly and effectively • supports AI adoption initiatives including environmental impact considerations.	• Evidence of supporting or guiding others to use AI tools responsibly and effectively • Contributions to AI adoption initiatives with environmental impact considerations documented	
Highly Advanced BSBDIG506X	Candidate: • develops and applies AI approaches and integration plans for complex, non-routine organisational challenges and leads initiatives that optimise AI use • applies and contributes to governance frameworks for AI implementation and output evaluation covering protection, privacy, security, bias, synthetic media, vendor assurance and regulatory requirements • leads responsible AI adoption initiatives applying ethical frameworks; applies human-centred AI practices maintaining appropriate oversight and critical thinking • leads initiatives building understanding of effective human-AI collaboration • develops capability-building programs for AI.	• AI integration plans or approaches developed for complex, non-routine organisational challenges, with leadership of implementation evidenced • Contributions to, or development of, AI governance frameworks covering protection, privacy, security, bias, synthetic media, vendor assurance and regulatory requirements • Responsible AI adoption initiatives led, with ethical frameworks applied and documented • Evidence of human-centred AI practices applied to maintain critical thinking and integrate human judgement across complex competing priorities • Initiatives led that built organisational understanding of effective human-AI collaboration • Capability-building programs developed and delivered supporting AI across a team or organisation	*"Describe an AI integration plan or approach you developed for a complex organisational challenge. How did you lead the initiative and what governance considerations shaped your decisions?"* *"Tell me about your contribution to an AI governance framework. What did you contribute, what requirements did it address, and how was it implemented?"* *"How have you led initiatives to build organisational understanding or capability in effective human-AI collaboration? What was your approach and what was the outcome?"*

DRAFT

2.2.7 Cyber Security

This digital capability area is about recognising and responding to cyber security risks and protecting workplace digital assets. It spans basic threat awareness through to strategic threat management and security governance leadership, aligned to the ASD Cyber Skills Framework and NIST CSF 2.0.

RPL candidates will typically have developed capability through:

- workplace cyber security training and awareness programs
- incident reporting and threat response activities
- security-aware digital practice
- roles with data classification, access control or security compliance responsibilities
- industry certification: ASD Cyber Skills pathway, CISSP, CompTIA Security+
- personal cyber security practice: password management, multi-factor authentication, phishing recognition.

Note: Industry certifications are strong indirect evidence for Cyber Security UoCs. Assessors should cross-reference certification content against the unit's Performance Evidence and Knowledge Evidence to confirm coverage before using as sole evidence of digital capability.

Level	What to look for	Evidence examples	Assessor prompts
Basic **BSBDIG207X**	Candidate: • recognises at least two common workplace cyber security threats and can describe their likely impact on organisational systems or information • completes routine tasks in line with workplace security policies and access controls • handles sensitive information in accordance with data classification, storage and sharing requirements • reports a suspected threat or incident through the correct workplace channel • can describe how individual behaviour contributes to workplace cyber security culture.	• Examples of identifying at least two common cyber security threats encountered at work, with impact on organisational systems described • Records of completing routine tasks in line with workplace security policies and access controls, confirmed by supervisor or system logs • Evidence of handling sensitive workplace information correctly — classification, storage and sharing procedures followed • A record of reporting a suspected threat or incident through the correct workplace channel using appropriate escalation pathways • A workplace example describing how own behaviour supports the organisation's cyber security culture	*"Tell me about two cyber security threats you have encountered or could encounter in your workplace. What impact could they have on your organisation's systems or information?"* *"Describe how you handle sensitive information at work. What classification, storage and sharing requirements do you follow?"* *"Have you ever reported a cyber security concern or incident at work? Walk me through what you did and who you contacted."*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
Intermediate BSBDIG307X	Candidate: • recognises and responds to at least two different common workplace cyber security threats using established procedures • applies workplace security procedures to protect digital systems, devices and information; applies appropriate access controls, secure storage and data handling procedures for sensitive information across varied contexts • reports security concerns and participates in incident response activities; contributes to workplace security awareness or shares security knowledge with colleagues to support a positive security culture.	• Examples of recognising and responding to at least two different cyber security threats using established workplace procedures • Records of applying access controls, secure storage methods and data handling procedures across varied workplace contexts • Evidence of reporting a security concern and participating in incident response activities, with steps taken documented • Contributions to a workplace security awareness activity or records of sharing security knowledge with at least one colleague • Supervisor confirmation that security procedures were applied correctly and consistently across different situations	*"Describe two different cyber security threats you have encountered and how you responded to each using your workplace procedures."* *"Tell me about how you apply access controls and data handling procedures for sensitive information in your role. How do these vary across different contexts?"* *"Have you contributed to a security awareness activity or helped a colleague understand a security practice? What did you do and what was the outcome?"*
Advanced BSBDIG407X	Candidate: • identifies and assesses at least three different cyber security threats; evaluates risk levels and advises colleagues on protective responses • implements, monitors and systematically reviews security measures; promotes safe security practices • protects workplace data and maintains privacy standards; coordinates data protection compliance initiatives • coordinates cyber security incident response and recovery • communicates with stakeholders during security events; reviews incident outcomes	• Risk assessments identifying and evaluating at least three different cyber security threats with recommended protective responses • Records of implementing, monitoring and reviewing security measures across workplace systems • Evidence of coordinating data protection compliance or privacy initiatives in a workplace context • Incident response coordination records including stakeholder communication during a security event and post-incident review outcomes	*"Describe a time you identified and assessed multiple cyber security threats in your workplace. How did you evaluate the risk levels and what did you advise?"* *"Tell me about a cyber security incident you coordinated a response to. How did you manage stakeholder communication and what improvements resulted from the review?"* *"How have you contributed to building cyber security capability or culture in your organisation?*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	and supports improvements to incident management • promotes security awareness and contributes to programs building sustainable cyber security capability.	• Security awareness initiatives promoted or contributed to, with evidence of impact on colleague engagement • Contributions to programs building sustainable cyber security capability within a team or organisation	*What approaches have you used?"*
Highly Advanced BSBDIG507X	Candidate: • develops and applies integrated threat management approaches incorporating security intelligence and emerging technologies • critically evaluates cyber security technologies and threat intelligence to inform strategic decision-making • develops and applies data security frameworks incorporating privacy governance and compliance mechanisms • critically evaluates developments in data security, privacy governance and regulatory compliance for strategic implications • leads, evaluates and continuously improves incident response frameworks • applies and contributes to security culture and governance frameworks • builds cyber security capability in others; critically evaluates security culture models to direct strategic implementation.	• Integrated threat management approaches developed and applied incorporating security intelligence and emerging technologies • Critical evaluations of cyber security technologies or threat intelligence informing strategic organisational decisions • Data security frameworks developed incorporating privacy governance and compliance mechanisms, with regulatory implications assessed • Incident response frameworks led, evaluated and continuously improved, including communication protocols and recovery strategies • Contributions to security culture or governance frameworks with strategic implementation directed across the organisation • Capability-building programs led or mentoring provided to develop cyber security capability in others	*"Describe an integrated threat management approach you have developed. How did you incorporate security intelligence and emerging technologies, and what strategic decisions did it inform?"* *"Tell me about a data security or privacy governance framework you have developed or contributed to. How did you assess its regulatory implications and how was it implemented?"* *"How have you led the evaluation and continuous improvement of an incident response framework? What did the review find and what changes resulted?"*

DRAFT

2.2.8 Digital Skills in the Workplace

This competence area integrates capabilities across all digital capability areas — information search and management, communication and collaboration, content creation, safety and wellbeing, and problem-solving — applied together in authentic workplace contexts. It is designed for learners who apply digital skills in an integrated, cross-functional way rather than within a single competence area.

RPL candidates will typically have developed capability through:

- roles requiring the regular use of multiple digital tools and platforms across different workplace functions
- participation in digital communication and collaboration activities as part of everyday work
- creating, modifying or managing digital content in line with workplace procedures and quality standards
- following workplace security, privacy and wellbeing practices as part of routine digital activity
- identifying and resolving common technical problems encountered during digital workplace tasks
- supporting colleagues or teams to use digital tools effectively across more than one digital capability area.

Level	What to look for	Evidence examples	Assessor prompts
Basic BSBDIG208X	Candidate: • accesses, searches and organises workplace information using digital systems and stores files following workplace procedures • participates in digital tasks requiring both interaction through workplace communication tools and contribution to a shared collaborative activity • creates and modifies basic digital content using workplace tools and templates • follows security, privacy and wellbeing practices • recognises and resolves technical problems using troubleshooting procedures, digital assistance tools and escalation pathways.	• Examples of accessing, searching and organising workplace information using digital systems, with files stored following workplace procedures • Records of participating in a digital communication or collaboration activity applying organisational conventions • Basic digital content created or modified using workplace tools and templates, such as a document, form or presentation • Evidence of following security, privacy and wellbeing practices during digital workplace activities • A record of identifying and resolving at least one common technical problem using	*"Walk me through a typical day using digital tools at work. Which systems do you use, what tasks do you perform, and how do you follow your workplace's procedures?"* *"Tell me about a time you participated in a digital collaboration activity at work. What was your role and how did you apply your organisation's conventions for sharing information?"* *"Describe a technical problem you have encountered during a workplace digital task. How did you identify it and what steps did you take to resolve it?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
		troubleshooting procedures or escalation pathways	
Intermediate BSBDIG308X	Candidate: • conducts and documents targeted information searches with source evaluation • coordinates and contributes to digital communication and collaboration across platforms with ethical information sharing • creates and edits digital content across different formats meeting accessibility and audience requirements with ethical AI interaction • implements security threat prevention and privacy measures and adapts digital usage in response to wellbeing considerations • resolves technical problems and adjusts digital environment settings to meet personal or others' needs.	• Documented targeted information searches showing how sources were evaluated for credibility and organised for workplace use • Records of coordinating or contributing to digital communication and collaboration across at least two different tools or platforms • At least two digital content items created or edited across different formats, addressing accessibility and audience requirements with AI disclosure documented where applicable • Evidence of implementing security threat prevention and privacy measures and adapting digital usage in response to wellbeing or harmful content considerations • A documented technical problem resolution with digital environment settings adjusted as needed	*"Describe a workplace task that required you to search for, evaluate and organise information digitally. How did you assess source credibility and how did you document your approach?"* *"Tell me about a time you coordinated or contributed to a digital collaboration activity across more than one platform. How did you manage ethical information sharing?"* *"Walk me through a content creation task where you needed to address accessibility, audience requirements and AI use. How did you approach each of those considerations?"*
Advanced BSBDIG408X	Candidate: • implements advanced information search and evaluation methods and applies ethical data management to support decision-making • coordinates ethical digital communication and collaboration using integrated tools and supports others to build collaboration capability	• Advanced information search and evaluation methods implemented with ethical data management applied to support workplace decision-making • Records of coordinating ethical digital communication and collaboration across integrated tools, including supporting others to build capability	*"Describe a workplace task where you needed to apply advanced digital skills across multiple digital capability areas. How did you manage the integrated requirements?"* *"Tell me about how you have supported others to develop their integrated digital capability. What approach did you take and what was the outcome?"*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	• creates specialised digital content using ethical AI practices and applies computational thinking and automation • implements cyber security, privacy, wellbeing and sustainability practices • diagnoses and resolves technical problems using human-centric approaches • supports and guides others in developing integrated digital capability • evaluates digital technologies for accessibility, inclusivity, fairness, rights-sensitivity and democratic impact.	• Specialised digital content created using ethical AI practices, with computational thinking or automation tools applied • Evidence of implementing cyber security, privacy, wellbeing and sustainability practices in an integrated workplace context • Technical problem diagnoses and resolutions using human-centric approaches, with guidance provided to others • Evaluations of digital technologies for accessibility, inclusivity, fairness, rights-sensitivity or democratic impact, with outcomes documented	*"How have you evaluated a digital technology for its accessibility, inclusivity or democratic impact in your workplace? What did you find and what action resulted?"*
Highly Advanced BSBDIG508X	Candidate: • develops and applies integrated digital approaches combining information management, communication, content creation, safety and problem-solving at a strategic level • assesses developments across all digital capability areas including emerging technologies • leads or contributes to integration initiatives spanning multiple digital capability areas including automation, AI and complex problem-solving requiring strategic judgement • develops and applies approaches to complex cross-competence challenges	• Integrated digital approaches developed and applied combining capabilities across multiple digital capability areas at a strategic organisational level • Assessments of emerging developments across digital capability areas informing organisational strategy • Integration initiatives led or contributed to spanning multiple digital capability areas, including automation, AI or complex problem-solving with strategic judgement applied • Complex cross-competence challenges addressed through advanced design, data visualisation, content integration, cyber security leadership or tailored digital solutions • Organisational capability built through mentoring, learning resource development,	*"Describe an initiative you have led that required integrating advanced digital capabilities across multiple digital capability areas. How did you develop the approach and what strategic judgements did you make?"* *"Tell me how you assess emerging developments across digital capability areas to inform your organisation's direction. Give me a specific example of how that assessment shaped a decision or initiative."* *"How have you built organisational digital capability across multiple digital capability areas? What combination of*

DRAFT

Level	What to look for	Evidence examples	Assessor prompts
	• builds organisational capability through mentoring, learning resource development, ethical and inclusive practice promotion, and digital behaviour policy leadership.	ethical and inclusive practice promotion, and digital behaviour policy implementation	*mentoring, resource development or policy leadership have you applied?"*

DRAFT

2.3 Priority Cohort Guidance

The Digital Capability UoCs serve a broad and diverse population of Australian workers. RTOs must ensure that RPL processes are genuinely accessible and do not create systemic disadvantage for learners from priority cohorts. This section provides specific guidance for four priority cohorts identified through the FSO Priority Cohort Consultation (2026).

Reasonable adjustment and flexibility apply equally to RPL and assessment-only pathways, as it does to training delivery and assessment. Adjustments must not alter the standard required for competence; it adjusts how competence is demonstrated, not the benchmark.

Cohort	RPL evidence considerations	Flexibility	Additional considerations
First Nations candidates	Community-based evidence including oral testimony, community project contributions and cultural digital practices may be submitted. A community Elder, respected person or Indigenous community organisation may act as a third-party verifier. Evidence of digital practice embedded in culture, land management, health or community service contexts is appropriate and valid.	Allow oral submission of self-evaluation. Offer assessor conversations in community settings or via video with cultural support person present. Allow extended evidence submission timelines. Avoid requiring written reflection if oral alternatives can demonstrate the same capability.	Apply Indigenous Data Sovereignty principles (CARE, OCCAAARS) when handling candidate data. Seek cultural advice before designing any community-based evidence collection. Part B S 6.3 for resources.
Candidates with disability	Reasonable adjustment applies to RPL evidence collection and assessment-only pathways equally. Candidates may use assistive technology artefacts as direct evidence. Evidence of digital capability demonstrated through adjusted means (screen reader use, voice input, switch access) is valid and should not be downgraded.	Adjust evidence submission format to match the candidate's access needs (audio, video, typed, scribed). Allow extended time for portfolio compilation. Provide accessible assessment interview formats. Assistive technology use is evidence of digital capability, not a gap.	Reasonable adjustment must not alter the standard required for competence – only the means of demonstrating it. Document all adjustments applied. Refer to Standards for RTOs 2025 and Disability Standards for Education / Disability Discrimination Act 1992 (Cth) for guidance on reasonable adjustment obligations.

DRAFT

Cohort	RPL evidence considerations	Flexibility	Additional considerations
Culturally and/or linguistically diverse (CALD) candidates	Candidates from CALD backgrounds may hold substantial digital capability developed in other national contexts, using different tools and platforms. This experience is valid evidence. Translated evidence, with verified translation, is acceptable. Interpreter support may be used during competency conversations.	Provide plain-language assessment materials. Allow interpreter use during assessor conversations. Accept evidence from international workplace contexts where equivalent standards apply. Where English literacy is a barrier, separate foundation skills support from competency assessment – a candidate may be competent digitally but require ACSF Reading or Writing support.	Do not conflate language difficulty with digital capability gap. CALD candidates may have higher digital capability than their English proficiency suggests. Refer to FSO Practice Guide: Diversity and Inclusion and ACSF guidance.
Candidates with low digital confidence or limited prior access	Candidates who have developed digital capability in informal or community contexts – including through family support roles, volunteering, or self-directed learning – may hold relevant capability without formal workplace evidence. Inferential assessment through structured conversation and short supplementary tasks is appropriate.	Weight assessor conversation and observation more heavily where artefact portfolios are limited. Use supplementary tasks that are low-stakes and workplace-relevant. Provide orientation to the RPL process in plain language before commencing. Allow portfolio compilation support (for example, assistance identifying and gathering evidence).	Low digital confidence is not the same as low digital capability. The RPL process itself should not create a digital access barrier – offer non-digital submission pathways where needed. Refer to Australian Digital Inclusion Index guidance and FSO Practice Guide: Diversity and Inclusion.

DRAFT

Section 3 – Resource Listing

The following resources support implementation of the Digital Capability UoCs. Resources are organised by category to assist RTOs, trainers, assessors and stakeholders in finding relevant material.

3.1 Key Frameworks and References

DigComp 3.0

Cosgrove, J. and Cachia, R. (2025). *DigComp 3.0: European Digital Competence Framework – Fifth Edition.* Publications Office of the European Union, Luxembourg. JRC144121.

The DigComp 3.0 publication is the key reference for this framework. It includes the five digital capability areas, 21 competencies, and four proficiency levels used in the Digital Capability units. The publication also includes a glossary of key terms supporting consistent interpretation across implementations.

Available from the JRC publications repository: https://publications.jrc.ec.europa.eu/repository/handle/JRC144121

Australian Qualifications Framework (AQF)

Australian Qualifications Framework Council. (2013). Australian Qualifications Framework, Second edition. AQF Council.

Provides AQF level descriptors used to calibrate the proficiency levels of the Digital Capability units (Basic = AQF 2, Intermediate = AQF 3, Advanced = AQF 4, Highly Advanced = AQF 5).

Available at: www.aqf.edu.au

Australian Core Skills Framework (ACSF)

Department of Industry, Innovation, Science, Research and Tertiary Education (DIISRTE) (2012). Provides the foundation skills reference framework underpinning the implicit foundation skills surfaced through the Digital Capability units. Used as the structural basis for Section 4 of Part B.

Available at: Australian Core Skills Framework (ACSF) - Department of Employment and Workplace Relations, Australian Government

3.2 VET Regulations and Standards

Training Package Organising Framework (TPOF)

The Training Package Organising Framework (effective 1 July 2025) sets out the Product and Process requirements that govern the design, development and endorsement of Training Package products, including the ASK template used in the Digital Capability units.

Available at: Training Package Organising Framework (effective 1 July 2025) - Department of Employment and Workplace Relations, Australian Government

Standards for Registered Training Organisations

Australian Skills Quality Authority. (2025). Standards for Registered Training Organisations (RTOs) 2025. Australian Government.

The Standards for RTOs apply to the delivery, assessment and quality assurance of all units, including the Digital Capability units. Practice Guides supporting the Standards (Assessment, Training, Recognition of Prior Learning, Trainer and Assessor Competencies, and others) provide additional guidance for RTOs implementing the framework. Further information at: Australian Skills Quality Authority

Qualifications Reform Design Group Final Report: Unlocking the Potential of VET

DRAFT

Establishes the Purpose 3 design principles applied to the Digital Capability units, supporting transferability and packaging flexibility.

Department of Employment and Workplace Relations. (2024). Qualifications Reform Design Group: Final report. Australian Government. Available at: Unlocking the Potential of VET

3.3 Indigenous Data Sovereignty Resources

The following resources support the application of Indigenous Data Sovereignty principles described in Part A Section 5.10. RTOs delivering Digital Capability units in First Nations contexts or where Indigenous data may be involved are encouraged to consult these sources.

Maiam nayri Wingara Indigenous Data Sovereignty Collective

The Collective's principles articulate community-led data governance, including the recognition of Indigenous data as a strategic Indigenous resource and the rights of Indigenous Peoples to determine the means of collection, access, analysis, interpretation, management, dissemination and reuse of Indigenous data. Available at Maiam Nayri Wingara

CARE Principles for Indigenous Data Governance

The Global Indigenous Data Alliance (GIDA) CARE Principles complement the FAIR Principles for data management and emphasise Collective benefit, Authority to control, Responsibility, and Ethics in Indigenous data work. Available at: The CARE Principles for Indigenous Data Governance – Global Indigenous Data Alliance

OCCAAARS Framework

The OCCAAARS framework articulates eight principles of Indigenous Data Sovereignty: Ownership, Control, Custodianship, Accessibility, Accountability to First Nations, Amplify the voices of the community, Relevant and reciprocal, Sustainability self-determining. Available at: OCCAAARS Presentation

3.4 Implementation Resources

Australian Government AI Policy and Guidance

The Australian Government has published guidance on AI use in the public sector and broader workplace contexts. RTOs delivering AI units may consult current policy through Australian Government channels. Available at: Policy for the responsible use of AI in government- Version 2.0 | digital.gov.au

Digital Inclusion Resources

The Australian Digital Inclusion Index (ADII) and related research from the Centre for Social Impact provide context on the digital inclusion landscape in Australia, supporting accessible, inclusive delivery of Digital Capability units. Available at: 2025 Australian Digital Inclusion Index

NCVER *Place-based and culturally responsive VET for Aboriginal and Torres Strait Islander learners* (May 2026).

The report:

- examines how RTOs can deliver better outcomes for First Nations learners through place-based delivery models and culturally responsive teaching,
- draws on case studies with three Aboriginal-led RTOs in urban (Tauondi College, Nunkuwarrin Yunti) and remote (Tiwi Islands Training and Employment Board) contexts.

https://www.ncver.edu.au/___data/assets/pdf_file/0030/9704136/Place-based-and-culturally-responsive-VET-for-Aboriginal-and-Torres-Strait-Islander-learners.pdf

DRAFT