



VISA 407 TRAINING PLAN – DIPLOMA OF COMMUNITY SERVICES (CHC52015) EQUIVALENT PROGRAM

1. PARTIES TO THIS AGREEMENT

Sponsor / Training Provider Company:

NetworkingCommunitiesCompany Pty Ltd

ABN: 21 128 348 863

Website: www.NetworkingCommunities.com

Gateway Platform: www.IDmatch.gov.au parallel use to Dept Home Affairs (Immigration)

Director: Michael Mattocks

Commonwealth Examiner – Cybersecurity & Digital Identity-

Apprenticeship www.WindHSE.org world 1st MA Cybersecurity Law (Latrobe University) – Network Security Fundamentals

Trainee Details

Full Name: _____

Country of Residence: _____

Address: _____

Mobile: _____

2. PROGRAM OVERVIEW

Structured occupational training under the Subclass 407 Training Visa, providing practical and theoretical training equivalent to Diploma of Community Services (CHC52015).

WORLD LEADING DIGITAL SAFEGUARDING & RISK AWARENESS (INTEGRATED COMPONENT)

(MyGov & NDIS Awareness Included)

A core component of this 24-month Subclass 407 Training Program is the integration of digital safeguarding, identity protection awareness, and information risk management within community services practice.

The trainee will develop structured awareness of risks affecting vulnerable individuals in digital and service environments, including:

- LinkedIn Partner Julie Inman Grant safety Commissioner
Worlds 1st age 16 social media age verification & restrictions
Phishing redirection and scam attempts targeting individuals
through email, SMS & voice recordings**
- LinkedIn partner Amanda Rishworth former NDIS Minister
now Minister Dept Employment MyGov accounts directives**
- impersonation risks involving government-style
communications, including MyGov-related scam activity and
fraudulent login attempts**
- awareness of identity theft risks affecting users of public
service systems and online government portals**

- **fraud risks within disability support environments, including NDIS-related service contexts, participant records, and invoice fraud risks**
- **safe handling of personal, sensitive, and client information in accordance with Australian Privacy Principles, ethical standards, and duty-of-care obligations**
- **recognition of heightened vulnerability among clients interacting with government or disability support systems online**
- **escalation procedures for suspected fraud, phishing, or identity compromise through appropriate organisational and official channels**

This component is delivered as risk awareness and safeguarding education within supervised workplace training, focusing on the identification, prevention, and escalation of potential digital threats impacting vulnerable populations.

The objective is to ensure trainees can recognise digital risks, respond appropriately within workplace procedures, and maintain confidentiality, ethical conduct, and professional standards in community services and disability support environments.

Delivery Methods:

- **On-the-job training in community services environments**
- **Hybrid online learning modules**
- **Competency-based assessments**

Mandatory Elective Component

Digital Identity Verification & eSafety Compliance (IDMatch) is included to support:

- **Identity verification processes**
 - **Compliance monitoring**
 - **Secure access to training environments**
 - **Fraud prevention and digital safety awareness**
-

Career Alignment Statement

This program develops advanced community services competencies aligned with workforce shortages in Australia.

3. TRAINING OBJECTIVES

The trainee will:

- **Apply Digital Privacy, safety, and compliance protocols**
 - **Complete IDMatch verification during induction and for suppliers/visitors**
 - **Apply identity verification, fraud awareness, and cybersecurity compliance practices**
-

4. TRAINING STRUCTURE

Duration: 24 months

Location: Australia

Delivery Model:

- On-the-job remote Training Sponsor observation & checklist in community services settings
- Hybrid online learning modules
- workplace rotations

Phase 1 (Months 1–6): Foundation Skills

- IDMatch verification for induction and access control
-

Phase 2 (Months 7–12): Core Practice

- Ongoing IDMatch verification for suppliers and visitors
-

Phase 3 (Months 13–18): Advanced Practice

- IDMatch verification maintained across all practical activities
-

Phase 4 (Months 19–24): Consolidation

- Continued IDMatch compliance integration
-

5. TRAINING OUTCOME SUMMARY

Category	Units
Core Units	12
Elective Units	8
Total Units	20 Units (CHC52015 Equivalent)

Category

Units

All to be Checklisted by Training

Sponsor

6. COMPLIANCE AND REGULATORY ALIGNMENT

This program complies with:

- **Subclass 407 occupational training requirements**
 - **Community Services industry standards**
 - **Australian Privacy Principles (APPs 1–13)**
 - **Work Health and Safety legislation**
 - **Duty of care and safeguarding frameworks**
 - **Cybersecurity and online safety awareness requirements**
 - **Mandatory IDMatch compliance tracking system**
-

7 VEVO / BRIDGING VISA JUSTIFICATION

- **Develop skills aligned with national workforce shortages**
 - **Maintain compliance through structured verification systems (IDMatch)**
 - **Bridging Visa with full working rights is advised**
-

Outcome:

**Certification equivalent to Diploma of Community Services
(CHC52015)**

8. SIGNATURES

Sponsor / Training Provider:

Michael Mattocks

TAE 40122

Signature: _____

Date: _____

Trainee:

Signature: _____

Date: _____
