

Emergency and Disaster Management Plan

Practice Name: Forge Clarity

ABN: 12685199124

Version: 1.0

Last Updated: November 2025

Next Review: December 2026

1. Practice Overview & Regulatory Context

Service Model: Remote telehealth counselling and therapeutic supports

Staff: Director/Lead Therapist (ACA/PACFA registered) + Volunteers (Thursday Zoom Grief Support Group only)

Clients: NDIS participants and general public (domestic and international)

Key Service: Individual therapy (Lead Therapist only); weekly public grief group (volunteers facilitate)

Regulatory Compliance:

- NDIS Practice Standards (Core Module + High Intensity Supports)
- NDIS (Incident Management and Reportable Incidents) Rules 2018
- Privacy Act 1988 & Australian Privacy Principles
- Health Records and Information Privacy Act 2002 (NSW)
- Work Health and Safety Act 2011 (NSW)
- ACA/PACFA Code of Ethics
- International jurisdictional requirements (per client location)

2. Risk Assessment Matrix

Emergency Type:

Likelihood:

Impact:

Priority:

Internet/tech failure during session:

High:

Medium-High:

Critical:

Client mental health crisis:

Medium:

Critical:

Power outage:

Medium:

High:

Client in immediate danger (DV/suicide):

Low-Medium:

Critical:

Practitioner illness/incapacitation:

Low:

High:

Cyber security/data breach:

Low:

High:

Critical:

Natural disaster:

Medium:

Medium-High:

High:

Platform outage (Zoom/Google):

Low:

Medium:

3. Client Safety Protocols

3.1 Emergency Contact Collection (Intake)

- Minimum one emergency contact with priority contact method (call/text/email)
- Client consent for emergency use (See the Client Liability Waiver & Agreement located: <https://forgeclarity.com.au/documents>)
- Current session location address if differs from usual is requested
- International emergency services: Primary 112 (universal mobile); country-specific researched

3.2 Client in Immediate Danger Response

If Client Responsive:

1. Maintain connection, conduct real-time safety planning
2. Contract for safety (if appropriate)
3. Identify immediate local supports
4. Schedule follow-up within 24 hours
5. Document immediately post-session

If Client Unresponsive or Imminent Danger:

1. 0-2 mins: Attempt contact via priority method (call/text/email)
2. Immediately: Call emergency services in client location:
 - Australia: 000 | International: 112
 - Provide: name, address, phone, situation

3. Simultaneously: Contact emergency contact persons
4. Within 2 hours: Confirm client safety, notify supervisor
5. Within 24 hours: Document with timestamps; NDIS Commission report (if participant and reportable)

3.3 Emergency Services Quick Reference

Australia:

- Emergency: 000
- Lifeline: 13 11 14 | Beyond Blue: 1300 224 636 | Suicide Call Back Service: 1300 659 467
- 1800RESPECT (DV): 1800 737 732
- Child Protection (NSW): 132 111

NDIS: 1800 035 544

International: 112 (universal mobile)

3.4 Vulnerable Client Safeguards

- Simplified communication options (visual cues for cognitive disabilities)
- Pre-session safety planning with support networks (upon request)
- Enhanced check-ins (mid-week contact as required/requested)
- Support coordinator collaboration (NDIS)

4. Technology & Infrastructure Contingencies

4.1 Backup Systems

Hardware: Primary laptop + 2 backup laptops | Battery packs (4-hour capacity) | Mobile hotspot (50GB data)

Platforms: Primary: Zoom | Backup: Google Meet → Teams → Phone call → Text messaging (crisis only)

Internet: Home broadband → Mobile hotspot → Alternative location (pre-identified)

4.2 Technology Failure Protocol

1. Minor glitch: Reconnect as soon as possible, continue session
2. Major disruption: Switch to backup platform (notify client via SMS), continue session
3. All tech fails: Phone safety check (high-risk clients within 30 mins); reschedule clients within 24 hours
4. Document disruption in clinical notes

4.3 Power Outage

- Activate battery pack + mobile hotspot
- Prioritize high-risk client sessions
- Reschedule non-urgent within 48 hours

4.4 Data Backup & Recovery

- Google Workspace: Automatic cloud backup, 2FA, 30-day version history
- Offline: Weekly encrypted backup to external hard drive (fireproof safe)
- Recovery: IT support response within 4 hours; RTO: 4 hours; RPO: 24 hours

4.5 Cybersecurity Breach Response

1. Immediate: Disconnect affected device
2. 30 mins: Change all passwords (secure device)
3. 2 hours: Contact IT support
4. 4 hours: Assess scope, identify affected clients
5. 24 hours: Notify affected clients; NDIS Commission (if participant data); OAIC (if serious harm likely)
6. 7 days: Professional indemnity insurer; ACA/PACFA

"Zoom-bombing" Prevention: Waiting room enabled, unique meeting IDs, password protection mandatory

5. Service Continuity Strategy

5.1 Response Levels

Note: All client notes are backed up online and these records are printed out once every six months to keep physical copies in the locked cabinet. The client code ledger is where client legal names are kept in a notebook that is kept in the locked cabinet.

Level 1 - Minor (tech glitch, brief outage):

Use backup systems; no broad notification needed

Level 2 - Moderate (1-3 day disruption):

Reschedule non-urgent; prioritise high-risk; phone check-ins; client notification within 4 hours

Level 3 - Significant (major disaster, extended incapacitation, cyber breach):

Emergency triage; high-risk safety checks within 4 hours; backup practitioner referrals; suspend grief group; NDIS Commission notification

Level 4 - Catastrophic (practice closure):

Executor activates closure protocol; immediate client referrals; NDIS/ACA/PACFA notification; records transfer as mandated (confidentiality is paramount and is kept as far as the law allows)

5.2 Essential vs Non-Essential Services

Essential (maintain except Level 4):

- High-risk client individual therapy (suicide risk, acute trauma, severe mental illness)
- NDIS complex therapeutic supports
- Crisis intervention
- Mandatory reporting follow-up

Non-Essential (postpone Levels 2-3):

- Grief Support Group
- Routine admin/billing
- New intakes (unless urgent)

- Low-risk maintenance sessions

5.3 Backup Practitioner Network

Identified practitioners with capacity for urgent referrals across specialisations (trauma, therapeutic supports, general counselling). Contact within 4 hours of need; warm handover if possible or requested.

5.4 NDIS Interim Behaviour Support Plans

As a 0128 provider we can not create interim behaviour support plans.

6. Staff Safety & Wellbeing

6.1 Director/Lead Therapist

Work-from-home safety: Ergonomic workspace, private session space, emergency exit access, first aid kit

Wellbeing: Monthly clinical supervision; peer support (ACA/PACFA); personal therapy as needed; immediate debriefing post-critical incident (within 48 hours); mandated supervision sessions as required per year

Sudden illness: Backup practitioner network activated (clients are given an option of practitioners to choose from); client notification as soon as possible (high-risk priority); automated out-of-office with backup contacts

6.2 Volunteers (Grief Group)

Requirements: Orientation (includes emergency protocols), WWCC/Police Check/NDIS Screening (if applicable), confidentiality agreement, Zoom security training

Session safety: Director on-call during group; co-facilitation (min 2 volunteers); participant safety check-in; host controls for disruptive participants

Wellbeing: Monthly debrief with Director; crisis debriefing access

7. Communication Plans

7.1 Client Notifications

Planned disruption (14 days notice): Email/SMS with backup practitioner referrals and rescheduling options

Emergency disruption:

- Within 4 hours: SMS/email to clients with appointments in next 48 hours
- Within 4 hours: Individual phone calls to high-risk clients
- Within 24 hours: Email to all active clients; website banner; social media (if appropriate)

Template:

"Due to [emergency], sessions are temporarily disrupted. Your [date/time] appointment is being rescheduled. I will contact you within [timeframe]. For urgent support: Lifeline 13 11 14. NDIS participants: your support coordinator has been notified."

7.2 NDIS Commission Reporting

Reportable incidents (within 24 hours): Death, serious injury, abuse/neglect, unauthorised restrictive practice, unexplained absence, incidents during emergencies

Method: NDIS Commission portal (www.ndiscommission.gov.au) or phone 1800 035 544

Service disruption >24 hours affecting NDIS supports: Notify within 24 hours with disruption details, duration, interim arrangements

7.3 Support Coordinator Communication (NDIS)

Email within 4 hours of disruption; daily updates during Level 3 (as required); collaborative interim planning (as required)

7.4 After-Hours Emergency Contact

High-risk clients with safety plans: Lead Therapist mobile [number]

All clients: Crisis services (Lifeline, Beyond Blue, 000/112)

8. Data Protection & Privacy

8.1 Storage & Security

- Google Workspace (encrypted, 2FA, APP-compliant)
- Offline encrypted backup (weekly, external drive, locked cabinet)
- Access: Director/Lead Therapist only
- Retention: 7 years post-service (NDIS + ACA/PACFA standard); international per client country requirements

8.2 Privacy Breach Response Timeline

30 mins: Contain breach as soon as possible | 2 hours: Assess scope | 4 hours: IT support engaged | 24 hours: Notify affected clients + NDIS Commission (if participant data) | 72 hours: OAIC (if notifiable breach) | 7 days: Insurer + ACA

9. Clinical Risk Management

9.1 High-Risk Client Enhanced Protocols During Disruptions

- Safety plan reviewed each session until resolved or client chooses to leave Forge Clarity
- Mid-week check-in (SMS/phone - upon request)
- Support network activated (GP, psychiatrist, support coordinator) with consent given by client / client nominated guardian
- Priority rescheduling within 24 hours if cancelled
- Alternative practitioner referral if disruption and if client requests >72 hours

9.2 Crisis Assessment Tools

- Suicidal Ideation Attributes Scale (SIDAS)

<http://nceph.anu.edu.au/research/tools-resources/suicidal-ideation-attributes-scale-sidas>

- Safety planning intervention (Stanley-Brown) - shared Google Doc

<https://suicidesafetyplan.com/>

- DV safe session environment confirmation; code word system, all client records and notes have a unique client code instead of their legal names. This is a safety measure to ensure that even if hacked, client confidentiality is maintained. Client names and the subsequent client codes are kept in a notebook that is kept in a locked cabinet.

9.3 Documentation Standards During Emergencies

- Session notes within 24 hours (standard) or 48 hours (major disruption)
- Emergency actions documented in real-time
- If full notes impossible: brief contemporaneous note immediately; full note within 7 days (flagged as "delayed due to emergency")

10. Financial & Administrative Continuity

Banking: Online/mobile app access from one device - the Director/Lead Therapists device

NDIS Billing: Portal accessible anywhere; Proda/RAM credentials in password manager;

phone/text/zoom/google teams sessions billable as telehealth if >30 mins

Scheduling: GoDaddy + Google Calendar (cloud-based); manual rescheduling if platforms down

Insurance Notifications:

- Professional Indemnity: 7 days (incidents potentially giving rise to claim)
- Business Insurance: 48 hours (property damage, cyber attack)

11. Training, Testing & Preparedness

11.1 Training Schedule

Director: Annual plan review (December) | Quarterly tech testing (Feb, May, Aug, Nov) | Annual first aid + cybersecurity training + ACA/PACFA required continued professional development training

Volunteers: Onboarding emergency training incorporated in Volunteer Liability Waiver for Volunteers

(<https://forgeclarity.com.au/volunteer> and <https://forgeclarity.com.au/documents>)

11.2 Testing Schedule

Monthly: Backup laptop check, battery charge, hotspot data

Quarterly: Full tech failover test, backup integrity, emergency contact currency

Annually: Tabletop exercise, insurance review, registration currency, plan update

11.3 Equipment Checklist

- ☐ Primary + 2 backup laptops (charged) | ☐ 2 battery packs (4-hour capacity) | ☐ Mobile hotspot |
- ☐ External backup drive (current <7 days) | ☐ Emergency contact list (printed + offline)

12. Recovery & Debriefing

Post-Incident Review (within 7 days): Document timeline, self-reflection, supervisor debrief, identify plan improvements, record lessons learned

Staff Support: Peer contact within 24 hours; clinical supervision within 48 hours; personal therapy as needed

Volunteer Support: Debrief within 7 days; individual check-ins offered upon request

Client Follow-Up:

High-risk: Phone within 24 hours, session within 48 hours, safety plan review

All active: Email within 7 days confirming restoration

NDIS: Support coordinator notification within 24 hours; Commission update

Service Restoration Priorities:

1. 0-24 hours: High-risk safety checks, resume essential services, notify stakeholders
2. 24-72 hours: Reschedule all appointments, resume grief group, process admin backlog
3. 1-2 weeks: Post-incident review, plan updates, return to normal operations

13. Legal & Compliance

13.1 Professional

Indemnity Insurance:

Policy: Berkley Insurance Company trading as Berkley Re Australia

ABN 53 126 559 706

Level 7, 321 Kent Street, Sydney NSW 2000

Policy: ACA421789

Effective: 19/05/2025 4.00 pm To: 19/05/2026 4.00pm

Coverage: Telehealth, interstate, international (confirm jurisdictions), cyber, contractual (NDIS)

Emergency notification: 7 days for potential claims

13.2 Mandatory Reporting (No Extension for Emergencies)

Child Protection (NSW 132 111): Within 24 hours of forming belief

NDIS Reportable Incidents: 24 hours (portal or phone 1800 035 544)

ACA/PACFA: As soon as practicable (aim 7 days)

13.3 Consent Requirements (Obtained at Intake)

- Emergency contact use
- Release to emergency services
- Support coordinator communication (NDIS)
- International jurisdictional practice
- Technology platforms and backups

13.4 Cross-Border Practice

Interstate: National registration (ACA/PACFA) covers all Australian states; state-specific mandatory reporting researched

International: Client informed Australian laws apply; local emergency services researched pre-session; mandatory reporting limitations documented; telehealth limitations discussed

14. Quick Reference Flowcharts

Client Unresponsive During Session

UNRESPONSIVE → Try re-engage (30 sec) → Attempt contact via priority method (2 mins)
 → No response? → Call 000/112 + emergency contacts → Document with timestamps
 → Supervisor notification (2 hours) → Follow-up safety confirmation (2 hours)
 → NDIS Commission if reportable → Clinical note (24 hours)

Technology Failure During Session

CONNECTION LOST → Wait 1 min → Reconnect same platform (2 mins) → Failed?
 → SMS/email: "Switching to [backup platform]" → Works? Continue session
 → Still failed? → Phone call → All tech failed? → Phone safety check (high-risk)
 → Reschedule within 24 hours → Document
 Client Immediate Danger (DV/Suicide)

IMMEDIATE DANGER DISCLOSED → Assess immediacy → Keep client on line
 → Safe to talk? Code word check → Can client call 000?
 → YES: Support to call | NO: You call 000 while maintaining contact
 → Stay connected until help arrives → Contact emergency contacts
 → Document with timestamps → NDIS/Mandatory reporting (24 hours)
 → Supervisor debrief (48 hours) → Follow-up (24 hours)

Cyber Security Breach

BREACH SUSPECTED → Disconnect device → Change passwords (30 mins, secure device)
 → Contact IT support (2 hours) → Assess scope (4 hours)
 → Notify clients + NDIS/OAIC (24 hours) → Insurer + ACA/PACFA (7 days)
 → Strengthen security → Post-incident review → Update plan

15. Emergency Contact Lists

Key Contacts

Clinical Supervisor:

Name: Debra Cowen

Email: debracowen@gmail.com

Professional Indemnity:

Insurer: Berkley Insurance Company trading as Berkley Re Australia

ABN 53 126 559 706

Level 7, 321 Kent Street, Sydney NSW 2000

Phone: 02 9275 8500

Policy #: ACA421789

Backup Practitioners (Urgent Referrals)

1. Name: Reuben McIntyre

Specialisation: Grief, Supervision, Drugs, Addiction, Wellbeing, Families, Couples

Website: <https://www.welcometobetter.com.au/meet-reuben>

Phone: (+61) 0481 114717

Email: reuben@welcometobetter.com.au

NDIS: Not

2. Name: Debra Cowen

Specialisation: Supervision, Grief, Training, Children, Teens, Families, Art Therapy

Phone: 0414 757 391

Email: debracowen@gmail.com

NDIS: Not

3. Name: Goal Coach

Specialisation: Online NDIS Counselling

Phone: 1300 190 377

Website: <https://goalcoach.com.au/ndis-counselling/>

Email: hello@goalcoach.com.au

NDIS: Yes

Platform Support

Zoom: support.zoom.us

Phone: Call 1.888.799.9666

Google Workspace: support.google.com/a

GoDaddy: 1300 351 076

16. Templates

Incident Report Template

Date/Time: _____ | Type: ☐ Tech ☐ Crisis ☐ Cyber ☐ Disaster ☐ Other

Level: ☐ 1 ☐ 2 ☐ 3 ☐ 4 | Client(s): _____ (NDIS: Y/N)

Actions Taken: [Timestamp] - [Action] (repeat)

Notifications: ☐ 000 ☐ Emergency contacts ☐ NDIS ☐ Support coordinator ☐ Supervisor ☐

ACA/PACFA ☐ Insurer

Outcome: [Client status, resolution time]

Lessons Learned: [What worked, what to improve, plan updates needed]

Completed by: _____ Date: _____ Reviewed with supervisor: _____

Client Safety Plan (High-Risk)

Name: _____ Date: _____ Review: _____

Warning signs: 1.____ 2.____ 3.____

Coping strategies: 1.____ 2.____ 3.____

People for help: 1.Name____ Phone____ 2.Name____ Phone____ 3.Name____ Phone____

Professionals: Therapist [your details] | GP____ | Psychiatrist____ | Support Coordinator____

Crisis services: Lifeline 13 11 14 | Beyond Blue 1300 224 636 | Emergency 000/112

Means restriction: _____

Reasons for living: 1.____ 2.____ 3.____

Emergency code word: ____ = "I am not safe"

Signatures: Client____ Date____ | Therapist____ Date____

17. Compliance Checklist

- ☐ NDIS Practice Standards 1.2, 2.1, 2.3, 4.1, 4.2, 5.1, 6.2 + High Intensity Supports (if applicable)
- ☐ NDIS Code of Conduct (respect, safety, integrity)
- ☐ Privacy Act 1988 / APPs 1, 6, 11, 12 + Notifiable Data Breach (72-hour reporting)
- ☐ WHS Act 2011 (NSW) - work-from-home safety
- ☐ ACA/PACFA Code of Ethics - duty of care, competence, confidentiality, boundaries, supervision

18. Plan Maintenance

Review Triggers: Annually (November) | Post-Level 3/4 incident (7 days) | Regulatory change (30 days) | Business change (30 days)

Version Control:

Version	Date	Changes	Approved
1.0	Nov 2025	Initial	[Director]

Storage: Google Drive > Business Documents > Emergency_Disaster_Management_Plan_v1.0.pdf

Access: Director (full) | Volunteers (relevant sections view-only) | Supervisor (on request)

Printed: One copy in home office; emergency sections visible near workspace

Staff Acknowledgment

All staff and volunteers sign an acknowledgement that they have read, understand, and will comply with this Emergency and Disaster Management Plan along with other relevant documents outlined here: <https://forgeclarity.com.au/documents> and <https://forgeclarity.com.au/volunteer>