

The ReConnect Programme – Business Continuity Plan

OWNERSHIP: The ReConnect Programme
AUTHORISED BY: Chief Operating Officer
REVIEW: August 2027

Purpose

The purpose of this plan is to protect young people, staff, visitors and partners, maintain safeguarding and welfare, and enable The ReConnect Programme to continue priority services during and after disruption.

Scope

This plan applies across The ReConnect Programme, including all employees, facilitators, mentors, volunteers, contractors, delivery partners and young people. It covers all ReConnect premises, satellite and community locations, outreach activity, transport, digital systems and supporting business functions.

Continuity commitment

The ReConnect Programme is committed to a safe, proportionate and trauma-informed response. Business disruption will not lower safeguarding standards, and delivery will not continue where staffing, premises, transport or other controls are unsafe.

Responsibilities

Chief Executive Officer (CEO) - overall incident authority, strategic decisions, closure or relocation, commissioner liaison and recovery approval.

Designated Safeguarding Lead (DSL) - safeguarding oversight, welfare prioritisation and statutory escalation throughout disruption.

Chief Operating Officer (COO) - operational continuity, site, staffing, transport and alternative-delivery coordination.

All staff - follow instructions, maintain supervision and accountability, report concerns promptly and keep accurate records.

PLAN

Document control and approval

Version	Date	Owner	Summary of change
1.0	May 2026	ReConnect Leadership	Initial detailed business continuity plan

Team

2.0	September 2026	CEO / COO	Merged and strengthened plan: network delivery model, activation levels, recovery targets, response checklists, decision log, exercise schedule and appendices
-----	----------------	-----------	--

Approval

Name	Role	Signature	Date
Chris Sodey	CEO		
Scott Gaskins	Safeguarding Lead		
Naomi Hamer	COO / Operations Lead		

Distribution and availability

Controlled digital copy in the central policy and continuity library.

Read-only remote copy accessible to the Business Continuity Team.

Site emergency pack containing this plan, key action cards and blank manual registers.

Confidential contacts, personal details, access codes and supplier account information maintained separately with restricted access.

Contents

1. Purpose, principles and scope
 2. Organisation and continuity model
 3. Governance, activation and command
 4. Critical functions and recovery priorities
 5. Communication and safeguarding continuity
 6. Incident response action cards
 7. Technology, information and records
 8. Premises, transport, people and suppliers
 9. Recovery, stand-down and lessons learned
 10. Training, testing and maintenance
- Appendices: quick actions, logs, contacts and checklists

1. Purpose, principles and scope

1.1 Purpose

This plan sets out how The ReConnect Programme will protect people, maintain safeguarding and continue priority services during and after disruption. It provides a consistent structure for assessment, decision-making, communication, temporary delivery and recovery.

- Protect young people, staff, visitors and partners.
- Maintain safeguarding and welfare without interruption.
- Minimise disruption to education, therapeutic support and engagement.
- Preserve access to essential records, communications and operational systems.
- Support a controlled, safe and timely return to normal delivery.
- Record decisions, impacts and learning so resilience improves after each event.

1.2 Continuity principles

Priority order: Life safety first; safeguarding and welfare second; stabilisation and communication third; continuity of provision fourth; full recovery and improvement fifth.

- Trauma-informed response: changes are explained clearly and individual regulation, attachment, sensory and communication needs are considered.
- Proportionate response: restrictions or closures are no wider or longer than necessary.
- Single source of truth: the Incident Lead authorises operational updates and the Administration Team records them.
- No unsafe continuity: delivery will not continue where staffing, premises, transport or safeguarding controls are inadequate.
- Commissioner partnership: referring schools, local authorities and involved agencies are kept informed of material changes.

1.3 Scope

This plan applies to all employees, facilitators, mentors, volunteers, contractors, delivery partners and young people connected with ReConnect. It covers Thurston Park, satellite and intervention spaces, community partner venues, temporary locations, transport, outreach, mobile delivery and remote or hybrid provision.

1.4 Risks within scope

Category	Examples
People and safeguarding	Serious safeguarding or behaviour incident; missing young person; significant absence; DSL unavailable; infectious disease
Premises and utilities	Fire; flood; structural damage; contamination; vandalism; loss of power, water, heating or access
Technology and information	Cyber attack; data breach; loss of internet, devices, MIS, safeguarding or communications systems

Delivery and transport	Vehicle failure; fuel shortage; unsafe routes; partner venue closure; external provider failure
External and strategic	Severe weather; national or regional emergency; civil disruption; financial or supplier failure; commissioner restrictions

2. Organisation and continuity model

ReConnect provides alternative and additional provision through academic, vocational, creative, therapeutic and physical-development activity, normally in 1:1 or small-group arrangements. Continuity planning recognises that disruption can affect attendance, emotional regulation, trust, engagement and longer-term outcomes.

2.1 Flexible network model

The organisation reduces reliance on a single building by using a connected delivery model. Subject to suitability, consent, commissioning arrangements and completed risk assessment, continuity may be provided through:

- Main hub and specialist strand spaces.
- Smaller satellite or intervention sites.
- School-based and community partner spaces.
- Vocational workshops, therapeutic and outdoor environments.
- Outreach, mobile delivery and adjusted transport routes.
- Remote mentoring, wellbeing contact, project work and online theory delivery.

Important: Remote delivery is a supportive continuity option, not an automatic substitute for meaningful in-person provision. Suitability must be considered for each young person and agreed with the referrer where required.

2.2 Conditions for an alternative venue

- A site-specific risk assessment and safeguarding arrangements are confirmed before use.
- Fire, first aid, welfare, accessibility, supervision and emergency procedures are adequate.
- The venue is appropriate to the individual young person and planned activity.
- Staff can securely access essential contact, risk, medical and safeguarding information.
- Attendance, session records, incidents and concerns are recorded under normal ReConnect procedures.
- Commissioner and parent/carers communications are completed where arrangements materially change.

2.3 Planning assumptions

- Some incidents will occur with little or no warning.
- Mobile networks or cloud systems may be temporarily unavailable.
- Not all young people can safely or effectively access remote learning.
- Staff and transport availability may reduce at the same time.

A disruption may affect one room, one site, several services or the wider locality.

Manual records and offline contact routes must therefore remain available.

3. Governance, activation and command

3.1 Business Continuity Team

Role	Core responsibility	Deputy / fallback
CEO / Incident Lead	Declares activation; strategic decisions; closure/relocation; commissioner and agency liaison; recovery authority	Nominated senior leader
Safeguarding Lead	Safeguarding oversight; welfare priorities; statutory escalation; access to safeguarding information	Deputy DSL
COO / Operations Lead	Impact assessment; site, staffing, transport and temporary delivery coordination; health and safety controls	Nominated operations manager
Administration Lead	Contact cascades; stakeholder updates; registers; incident and decision log; document control	Nominated administrator
IT / Data Lead	System containment, continuity, recovery and data-breach support	Approved IT support / senior lead
Tutors and practitioners	Follow instructions; maintain supervision, welfare contact, attendance and session reporting	Allocated line manager

3.2 Activation levels

Level	Trigger and impact	Authority and response
Level 1 - Local	Contained disruption; normal management arrangements remain effective	Relevant manager coordinates and logs actions; Incident Lead informed if impact may grow
Level 2 - Significant	One site/service unavailable, material staffing or system loss, or continuity arrangements required	CEO or delegated Incident Lead activates BCP; Business Continuity Team convened
Level 3 - Critical	Threat to life or safeguarding, multi-site/widespread disruption, prolonged closure or major reputational/regulatory impact	Emergency services first where needed; CEO leads strategic response and external liaison

3.3 Activation triggers

Immediate danger or a serious safeguarding concern.
Site cannot be occupied or essential utilities are unavailable.
Safe staffing, DSL coverage or supervision cannot be maintained.
Critical system or communication loss exceeds the recovery target.
Transport failure prevents safe access for a material number of young people.
A public authority, emergency service, landlord or commissioner imposes restrictions.
The likely impact cannot be controlled through routine procedures.

3.4 First 60 minutes

Protect life, provide first aid, call emergency services and evacuate or secure the area as required.
Account for young people, staff, visitors and vehicles; report anyone missing immediately.
Notify the DSL of safeguarding implications and preserve supervision.
Appoint the Incident Lead and establish a safe coordination point.
Record time, facts, decisions, owners and next review time in the incident log.
Assess people, premises, systems, transport, delivery and stakeholder impact.
Agree a holding message and notify priority audiences using approved channels.
Set the next review point, normally within 30 to 60 minutes during the acute phase.

3.5 Authority and records

Only the CEO, delegated Incident Lead or emergency services may authorise whole-site closure or reopening. Managers may stop an unsafe activity or evacuate an affected area immediately. The Incident Lead must ensure a contemporaneous incident log and decision log are maintained, including decisions not to escalate or notify.

4. Critical functions and recovery priorities

Priority	Critical function	Target maximum interruption	Minimum continuity arrangement
1	Life safety, safeguarding and welfare	None / immediate	DSL or deputy coverage; emergency contacts; supervision; welfare triage and statutory escalation
2	Staff coordination and accountability	Immediate	Phone cascade; manual staff and visitor register; named Incident Lead
3	Stakeholder communication	Initial holding update within 2 hours	Mobile/email route; contact lists; approved message and update schedule

4	Learner records and safeguarding information	Within 4 hours	Secure remote access or controlled offline emergency information
5	Attendance and welfare monitoring	Same working day	Manual register; welfare contact and escalation for unexplained absence
6	Educational and therapeutic delivery	Aim within 24-48 hours	Adjusted timetable, alternative venue, outreach or suitable remote contact
7	Referrals and placement administration	Within 3 working days	Prioritised secure inbox and manual tracker
8	Finance, payroll and essential purchasing	Within 5 working days	Authorised remote access and emergency payment controls

Targets: These are internal recovery targets, not a promise that every function will resume within the stated period. Safety, safeguarding, staff availability and external restrictions take precedence.

5. Communication and safeguarding continuity

5.1 Communication sequence

Audience	Owner	Minimum message
Staff and on-site teams	Incident Lead / Administration	Safety action, reporting location, delivery status, next update time
Parents and carers	Administration, authorised by Incident Lead	Impact on attendance/transport, immediate action, support route, next update
Referring schools and commissioners	CEO / delegated lead	Affected learners/services, safeguarding and continuity arrangements, expected review point
Emergency or statutory agencies	DSL / Incident Lead	Factual information required for response, referral or notification
Partners, suppliers and landlord	Operations Lead	Access, service requirement, containment and recovery actions
Public or media	CEO or nominated spokesperson only	Approved factual statement; no personal or safeguarding information

Methods may include telephone, SMS, email, Arbor, approved secure platforms, website updates and direct manager contact. WhatsApp may be used only within approved organisational arrangements and must not contain unnecessary personal or safeguarding information. If a channel is compromised, use an alternative verified route.

5.2 Safeguarding continuity

DSL and deputy DSL availability is maintained or an alternative competent lead is identified.

Safeguarding concerns continue to be recorded and escalated under the Safeguarding and Child Protection Policy.

Essential risk, medical, contact and safeguarding information remains securely accessible to authorised staff.

Young people at heightened risk are prioritised for welfare contact, supervision and multi-agency coordination.

Where face-to-face delivery is disrupted, a documented welfare-contact plan is agreed for each affected vulnerable learner.

Partner and temporary sites work under ReConnect safeguarding, conduct, reporting and quality-assurance expectations.

A reduced timetable, welfare visit, transport adjustment or alternative location is implemented only after individual risk and safeguarding review.

Safeguarding threshold: Business disruption does not lower safeguarding standards. If safe supervision, reporting or escalation cannot be maintained, the affected delivery must pause and the referrer and relevant agencies must be informed.

5.3 Attendance and welfare

Maintain a manual attendance record if the MIS is unavailable.

Confirm the location and responsible adult for every young person during relocation or evacuation.

Follow up unexplained absence on the same day under normal attendance and safeguarding procedures.

Record every welfare contact, attempted contact, concern and escalation.

Transfer manual records securely into the normal system once restored, avoiding duplicate or incomplete entries.

6. Incident response action cards

6.1 Fire, structural damage or unsafe premises

Phase	Actions
Immediate	Evacuate and account for everyone; call emergency services; give first aid; prevent re-entry; notify Incident Lead and DSL.
Continuity	Confirm closure boundary and duration; secure records/equipment only when safe; activate communications; assess alternative venue, outreach or suitable remote arrangements.

Recovery	Obtain competent inspection/clearance; liaise with landlord and insurer; review damage and remedial works; complete reopening checklist and phased return if appropriate.
----------	---

6.2 Severe weather, flooding or extreme temperature

Phase	Actions
Immediate	Monitor official warnings and local travel; assess site, routes, utilities and vulnerable individuals; stop travel or activity where unsafe.
Continuity	Use delayed/staggered attendance, adjusted routes, relocation, reduced delivery or suitable remote welfare/learning; maintain regular updates.
Recovery	Inspect site and access routes; clean or repair affected areas; confirm utilities and safe temperatures; communicate reopening.

6.3 Utility failure

- Identify scope and estimated restoration time; contact provider/landlord.
- Assess fire systems, lighting, heating, sanitation, food safety, communications and accessibility.
- Relocate or close affected activity if essential welfare or safety controls cannot be maintained.
- Protect refrigerated medicines or food where relevant and record disposals.
- Do not reopen until essential services and safety systems are confirmed.

6.4 ICT failure, cyber incident or data breach

Phase	Actions
Contain	Notify IT/Data Lead; disconnect affected devices or accounts if advised; do not delete evidence; change credentials through a trusted device where required.
Continue	Use manual registers and authorised alternative communications; prioritise access to safeguarding information; restrict sensitive processing to what is necessary.
Assess and notify	Start a breach/incident log; identify systems, people and data affected; escalate to senior leadership and assess reporting duties. A notifiable personal data breach must be reported to the ICO without undue delay and, where feasible, within 72 hours of awareness.

Recover	Restore from tested backups; reset access; validate data and system integrity; reconcile manual records; communicate safe restoration; complete post-incident review.
---------	---

6.5 Significant staff shortage or loss of DSL coverage

- Confirm actual availability, competencies, first-aid provision, supervision needs and DSL/deputy coverage.
- Redeploy suitable staff and pause lower-priority activity.
- Use approved sessional or partner staff only when required checks, induction and supervision are in place.
- Prioritise learners whose welfare or safeguarding needs make disruption most harmful.
- Reduce, relocate or cancel sessions where safe staffing cannot be maintained.
- Inform families, referrers and commissioners promptly of material changes.

6.6 Infectious disease outbreak

- Follow current UK Health Security Agency, NHS and government advice.
- Complete individual and activity risk assessments for clinically vulnerable people where needed.
- Apply proportionate hygiene, ventilation, cleaning and exclusion arrangements.
- Use flexible staffing, cohorts, adjusted timetables or suitable remote arrangements.
- Maintain safeguarding contact for absent or isolated young people.
- Plan a supported return, including wellbeing and re-engagement needs.

6.7 Serious safeguarding, behaviour or critical incident

- Make the area safe, maintain supervision, summon emergency services if necessary and notify the DSL immediately.
- Follow the relevant safeguarding, missing person, behaviour, first aid, restrictive intervention or critical incident procedure.
- Separate the incident from wider provision without isolating a young person unsafely.
- Preserve evidence and record facts, actions, witnesses and notifications.
- Coordinate communication with parent/carers, referrer, social care, police or other agencies as directed by the DSL.
- Debrief and support affected people; review risk assessments and support plans before return.

6.8 Transport disruption or vehicle incident

- Protect life, stop in a safe location, account for passengers and contact emergency services where required.
- Maintain appropriate supervision and do not leave young people unattended.
- Notify Operations and parents/carers/referrers using verified contact details.
- Use alternative approved vehicles, adjusted routes/times, local delivery or cancellation following risk assessment.

Record the incident and complete vehicle, insurance and safeguarding reporting requirements.

6.9 Loss of partner, supplier or funding-critical service

Confirm the affected service, contractual position, stock/capacity and likely duration.

Prioritise essential safeguarding, food, utilities, transport, IT and staffing dependencies.

Activate approved alternatives and authorisation controls; avoid unvetted emergency suppliers for regulated or safeguarding-sensitive work.

Inform commissioners where delivery, cost or placement terms may materially change.

Review longer-term viability through the leadership risk register and financial controls.

7. Technology, information and records

7.1 Resilience controls

Use secure cloud services, role-based permissions, multifactor authentication where available and managed devices.

Maintain tested backup and restoration arrangements for critical information.

Keep a controlled offline emergency pack with minimum necessary contacts and action forms.

Review leavers, privileged access, shared accounts and third-party access promptly.

Ensure staff know how to report phishing, device loss, unauthorised access and data breaches.

Maintain a paper-to-system reconciliation process for outages.

7.2 Information handling during disruption

Use only the minimum personal information necessary for the response.

Verify recipients before sending sensitive updates.

Do not use personal email, unapproved storage or public messaging for safeguarding information.

Keep factual incident and decision logs; distinguish confirmed facts from assumptions.

Secure paper records and dispose of duplicates confidentially after reconciliation.

Follow the Data Protection Policy and retain evidence of breach-risk assessment and notification decisions.

7.3 Minimum offline pack

Item	Control
This BCP and action cards	Current controlled copy; reviewed termly
Blank attendance, incident and decision logs	Numbered/dated on use; transferred securely after recovery
Priority contact routes	Restricted, encrypted or sealed; minimum necessary information

Site plans and evacuation information	Available to Incident Lead and emergency services
Key learner emergency information	Risk-based minimum dataset; access logged and reviewed
Charged phone/power bank and stationery	Checked routinely

8. Premises, transport, people and suppliers

8.1 Preventive controls

- Fire, electrical, equipment, water, security and health and safety checks are maintained.
- Alternative venues and mutual-aid arrangements are identified in advance where practicable.
- Staff are cross-trained for essential administrative and operational roles.
- Vehicle, driver, insurance and maintenance records are current.
- Critical suppliers and IT support have escalation contacts and reasonable fallback arrangements.
- First aid equipment, emergency lighting, communication devices and chargers are checked.

8.2 Staffing continuity rules

Competence, vetting, safeguarding, supervision and risk controls apply during continuity arrangements exactly as they do in normal operation. Senior leaders may redistribute duties, but staff must not undertake work beyond their competence or authorisation. Staff wellbeing, fatigue and exposure to distress must be actively monitored during prolonged incidents.

8.3 Transport continuity rules

Transport changes must be authorised through Operations and communicated to the responsible adult and referrer where applicable. Any alternative vehicle, driver, pickup point, route or supervision arrangement must meet normal ReConnect transport, safeguarding and insurance requirements.

9. Recovery, stand-down and lessons learned

9.1 Recovery stages

Stage	Objective	Evidence required
1 - Stabilise	Safety, safeguarding, accountability and command established	Incident log; attendance/accountability; initial impact assessment
2 - Temporary operation	Priority functions delivered through controlled alternatives	Risk assessments; staffing plan; stakeholder updates; manual records
3 - Restore	Systems, premises and timetables returned safely	Technical/site clearance; data reconciliation; reopening checklist

4 - Improve	Learning embedded and residual risks managed	Debrief; action plan; policy/risk updates; commissioner feedback where relevant
-------------	--	---

9.2 Reopening and stand-down criteria

The immediate hazard is removed or controlled and any competent authority clearance is obtained.

Safeguarding, staffing, first aid, premises, transport and communication controls are adequate.

Critical systems or authorised workarounds are functioning and manual records can be reconciled.

Affected young people have individual return, regulation and support needs considered.

Parents/carers, staff, referrers and partners receive clear reopening arrangements.

The Incident Lead records the stand-down decision, remaining actions and monitoring period.

9.3 Post-incident review

A hot debrief should normally occur within 24 to 72 hours, followed by a proportionate formal review within 10 working days. The review must consider what happened, impact, safeguarding, decisions, communications, equality and accessibility, staff wellbeing, records, costs, recovery performance and lessons learned.

Action	Owner	Due date	Status / evidence

10. Training, testing and maintenance

10.1 Minimum programme

Activity	Frequency	Owner / evidence
Staff business-continuity awareness and induction	At induction and annual refresher	COO; attendance and learning record
Fire and evacuation drills	In line with fire risk assessment and procedures	Health & Safety Lead; drill record
Contact list and offline pack check	Termly	Administration Lead; signed checklist
Tabletop exercise: site loss or severe weather	At least annually	Business Continuity Team; exercise report
Cyber/data incident exercise and restore test	At least annually / supplier schedule	IT/Data Lead; test outcome and actions

Full plan review

Termly and after activation/material change Document Owner; document control update

10.2 Review inputs

Changes to sites, staffing, learners, services or delivery model.

New or changed legislation, safeguarding guidance, public health advice or commissioner requirements.

Exercise outcomes, incidents, near misses, complaints and feedback.

Changes in systems, suppliers, vehicles, insurance, contracts or emergency contacts.

Risk assessments, audits and assurance activity.

Appendix A - Immediate action checklist

Time	Check
0-15 min	Protect life; call emergency services; evacuate/secure; account for everyone; notify DSL and senior lead.
15-30 min	Appoint Incident Lead; open logs; confirm facts and impact; establish coordination point and next review.
30-60 min	Choose activation level; protect records; approve holding messages; plan staffing, transport and continuity.
1-2 hours	Notify priority stakeholders; agree arrangements for each affected young person; establish update rhythm.
Same day	Maintain safeguarding and attendance; record costs/decisions; review risk; plan next operational period.
Recovery	Validate safety and systems; reconcile records; authorise reopening; debrief and assign improvements.

Appendix B - Incident and decision log

Incident title: _____ Date opened: _____ Incident Lead: _____

Time	Information / event	Decision or action	Owner	Completed
------	---------------------	--------------------	-------	-----------

Appendix C - Initial impact assessment

Area	Status / impact	Immediate control	Further action / owner
People and accountability			
Safeguarding and welfare			
Premises and utilities			
Staffing and competencies			
Transport and access			
IT, data and communications			
Delivery and individual learners			
Partners, suppliers and finance			

Appendix D - Emergency contacts register

Confidentiality: Maintain this register separately or complete only in the restricted controlled copy. Check it termly and after staffing, supplier or site changes.

Function / organisation	Primary contact	Fallback / out-of-hours	Last checked
Emergency services	999 / 112	Police non-emergency: 101	
CEO / Incident Lead			

Safeguarding Lead /

Deputy DSL

COO / Operations

IT support / cyber
response

Landlord / building
management

Electricity / gas / water

Insurance provider / broker

Suffolk safeguarding /
social care route

Approved alternative
venue 1

Approved alternative
venue 2

Transport recovery /
vehicle provider

Appendix E - Reopening checklist

- ☐ Competent clearance/inspection received where needed.
- ☐ Fire alarm, emergency lighting, exits, utilities, sanitation and security confirmed.
- ☐ First aid, medication and welfare arrangements confirmed.
- ☐ Safe staffing, DSL coverage and supervision confirmed.
- ☐ Systems restored or authorised workarounds in place.
- ☐ Manual attendance, safeguarding and operational records reconciled.
- ☐ Transport routes, vehicles and collection arrangements confirmed.
- ☐ Individual learner risk/support arrangements reviewed.
- ☐ Staff, parents/carers, referrers and partners notified.
- ☐ Incident Lead has signed the reopening and stand-down decision.

Authorised by: _____ Role: _____ Date/time: _____

Appendix F - Related documents and reference points

Safeguarding and Child Protection Policy

Health and Safety Policy and site risk assessments
Fire Safety Policy and evacuation procedures
Critical Incident Procedure
Data Protection and Information Security Policies
Online Safety Policy
First Aid Policy
Lone Working Policy
Transport Procedures
Educational Visits Procedures
Staff Code of Conduct and Staff Handbook
Individual risk assessments, support plans and emergency information

External reference points

The plan reflects current UK business-continuity principles and official incident-response expectations. It should be reviewed against current guidance when activated or updated.

Cabinet Office - Preparation and planning for emergencies -

<https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others>

National Cyber Security Centre - Cyber incident response guidance -

<https://www.ncsc.gov.uk/section/about-ncsc/incident-management>

Information Commissioner's Office - Personal data breaches -

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

VERSION CONTROL

We will review our documentation regularly and we reserve the right to amend our policies and procedures at any time.

Version	Date	Change Summary	Author/ Reviewer	Approved by:
1	26/08/26	Initial version	Naomi Hamer	Director