

Ginger Nut Training.



Document Title

Continuity of Apprenticeship Training

Originator

Director

Responsible Person

Director

Date of Approval

August 2026

Policy Due for Renewal

August 2027

Version

1.2

ginger**nut**[®]

Introduction

Ginger Nut Training acknowledge that there are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential disaster	Probability rating	Impact rating	Potential consequences and remedial actions
Flood	4	3	Ground floor office all PCs raised. All PCs backed up and replaceable with laptops. Risk of power cut, potential to close office. Staff to take laptops and work from home.
Pandemic	1	3	Office closed and all staff to work remotely and via cloud-based software.
Fire	3	2	Fire and smoke detectors on all floors. No chance of not hearing during working hours. Risk of closure of office and loss of equipment. Key staff to access off-site backup laptops and replacement equipment to be purchased and installed within 72hrs.
Electrical Outage	3	3	Loss of power reduces ability to use office equipment. Availability of remote working reduces impact
Act of terrorism	5	2	Office likely to become unavailable / unusable (switch to remote working). Potential loss of life – no real mitigation but grief counselling / other mental health support for staff, plus cross-training and written procedures to make it easier to cover where required.
Cyber attack	2	2	Potential loss of confidential data or access to systems
Loss of communications	3	3	All communications run on fibre. Where downtime occurs, mobile hotspots available as backup. If longer term outage then work from home available and all staff have access to mobile devices for calls.
Extreme weather	2	3	Extreme heatwave might make it too hot to work (office or WFH) without air conditioning or other mitigation. Other extreme conditions might make travel or locations unsafe.
Loss of access to critical systems	5	1	See IT sections below. A prolonged outage of core systems could cause a significant issue, but this is unlikely due to the backup and redundancies they have. Should this happen, the effects are unlikely to be confined to Ginger Nut, so expectations (client, learner, government etc) would probably be adjusted to compensate.

Probability: 1=Very High, 5=Very Low

Impact: 1=Total Shutdown, 5=Minor Inconvenience

Apprenticeships Training Programme delivery

Training Programmes are delivered remotely to staff either on employers' own premises or at home, so depending on the type of emergency/ hazard disruption may not be an issue. All training is delivered remotely so disruption would be if a learner was unable to access equipment through employer-based issues.

Due to the Coronavirus pandemic all training is delivered remotely so location of learners and tutors does not impact ability to train, where learners have access to appropriate equipment. Where this occurs in the

short term, impact will be minimal but for longer term (4 weeks or more) disruption Breaks in learning may be required.

The impact of a delay to training learners could be:

- A slowing down of progress towards the qualification
- Progression target dates and completion may be missed
- If completion targets are missed our success rates will be affected
- Potential effect future contracting agreements with the DWP or other funding bodies

Potential impact / timescales:

- First 24 hours – No impact
- 24-48 Hours – Minimal Impact
- Up to 1 week – Some impact
- 2- 4 weeks – Noticeable impact
- 4 weeks- maximum tolerable period of disruption before serious impact on success rates and reputation. Breaks in learning to be instigated.

To minimise serious impact, in the instance of long-term inability to visit learners, Ginger Nut Training would liaise with the DWP or other relevant funding bodies to discuss alternative options to support learners.

Ginger Nut Training are acutely aware of the impact to learners should any changes occur as follows and would aim to reduce the impact on the learners' progression.

IT Systems at Ginger Nut Training

All major systems are cloud based:

- Monday.com – Customer Contact management. Cloud only and in majority of cases have contacts separately in email and phones
- Monday.com – task management for client, delivery and enrolment teams. Short term disruption would be minimal but long term would affect efficiency of business.
- OneFile – cloud only, copies most comms and evidence locally too. High disruption to learning if offline for over 1 week but less short-term impact if down
- Microsoft Office 365 – main platform for email, servers, Teams and most office functions
- Cognisoft Yeti – ILR funding submission tool. Potential severe disruption if unavailable for a significant period, especially around funding submission deadlines, but manual workarounds available and any serious issues are likely to be industry-wide, which would probably lead to a government response to alleviate issues
- Xero – finance and accounting tool. Significant issues if unavailable for the long term, but manual workarounds available.
- Email – local storage on PCs and cloud-based access
- Server – SharePoint keeps regular files local and cloud based. External backup maintained for 186 days. Longer term disruption if lost for historic files which are rarely accessed. Short term lower impact.
- File backup – local documents, desktop etc backed up into cloud

- Docuware – enrolment system. Would require temporary delays to enrolment of learners. Longer term downtime would require switch to backup process using Monday/spreadsheet based management.
- Internet – We have a dedicated line so if that goes down can access separate Wi-Fi throughout building (separate channel). If both lines down, then revert to mobile 4G/5G hotspots
- Offsite working available, all data accessible remotely
- Computer/laptop theft or destruction – PCs are encrypted, all files backed up on cloud.

Communications Systems

Communications systems are predominantly cloud based and as such there is significant overlap with plans above. In addition to these:

- Main office phone system down - All staff have mobiles and using remote and local systems we can redirect line to Need More Time phone remotely for call filtering and message-taking.
- Mobile phone outage – all company mobiles are on the O2 network so if this went down there would be disruption. Office based staff are able to access phone system via desktop or laptop as required. All learners, clients and other contacts should have the main office number so calls can be received and in the majority of cases staff have a personal phone that can be used at short notice. Where this is not the case, we can purchase a phone and new SIM very quickly and use that until the network is back up and running.

Building

Business premises may be disrupted due to events outside of our control, such as:

- Fire
- Power / Water failure
- Failure of Heating Services
- Severe snow or other hazardous weather conditions preventing access
- Serious Security risk

Where the premises are unsafe for staff to attend, all staff will work from until further notice. All IT systems etc can be accessed remotely and business would continue.

If building destroyed, then a risk of loss of hard copies of paperwork but all originals are scanned and uploaded so recoverable. Loss of equipment would cause disruption but can be worked around.

Key staff, such as those who are part of the Crisis Management Team, maybe called upon to attend to oversee remedial actions. The role of the crisis team is to keep the business running as smoothly as possible and to liaise/inform stakeholders/ ESFA / HSE / Police etc regarding emergency plans.

Training is conducted remotely / via webinar / online so can continue with no adjustment.

Staffing issues

There will be occasions where a gap in staffing through natural turnover and Ginger Nut Training aim to minimise any negative impact on learners by:

- Ensuring assessing staff have transferable skills to be able to cover more than one vocational area
- Succession planning
- Some members of senior management team are qualified Apprenticeship Support Tutors who can temporarily support learners

Financial issues

The aim of the business is to ensure 'business as usual' should any funding streams be withdrawn. To do this, Ginger Nut Training's strategic aims are to have multiple income streams to negate risk.

- Diversification of client base, to reduce reliance on a few key clients
- Build reserves to maintain operations in short term
- Maintain a high credit rating to enable access to loans, temporary borrowing capability
- Commercial training (should the opportunity arise)
- Legal action where necessary (bad debts, reputational damage etc)

Transport issues

Where it is not possible to reach the office due to travel issues in or out of that office then all staff can work from home. Where staff are not able to access company equipment then disruption may occur and dispensation to use personal equipment can be sought from Harry Simpson, director, in consultation with TCS.

Disaster Recovery Team

The team will be contacted and assembled by the Emergency Response Team (ERT). The team's responsibilities include:

- Establish facilities for an emergency level of service within 2 business hours;
- Restore key services within 4 business hours of the incident;
- Recover to business as usual within 8 to 24 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.
- Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure

that communications can be quickly established while activating disaster recovery. The Disaster Recovery plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team:

- Harry Simpson – 07860 590 568
- Tanya Murphy – 07702 887 499
- Dan Williams - 07834 554 379

If not available try Phil Warnock – 07754 800510

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble online or in-person and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

Procedures for management

Members of the management team will keep contact details for each employee in their departments. In addition, management team members will have a local copy of the company's disaster recovery and business continuity plans on file in the event that the headquarters building is inaccessible, unusable, or destroyed.

Contact with employees



Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

Backup staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

Updates

For the latest information on the disaster and the organization's response, staff members can call any member of the ERT or BRT. Included in the exchanges will be data on the nature of the disaster, assembly sites, and updates on work resumption.

Personnel and family notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

Emergency contacts

Function	Company	Main Contact	Alternative contact
IT Support (inc. equipment & Microsoft)	TCS	Peter Rogers 01206 576043 pete@tcssupport.co.uk	support@tcssupport.co.uk 01206 570003
Broadband & Phones	County Broadband	Howard Lowe 07824 429 303 howardlowe@colchester-fibre.co.uk	support@myaccount.colchester-fibre.co.uk https://myaccount.colchester-fibre.co.uk/supporttickets.php
Learner records	OneFile	Michael Horton 0161 638 3876 Michael.Horton@onefile.co.uk	support@onefile.co.uk 0161 638 3876
CRM & task management	Monday.com	Caroline Morrison carolinemo@monday.com	Via support window at https://gingernutmedia.monday.com/
Building	Space	Jack Briggs-Miller 07817 000 953 colchesterteam@spacestudios.org.uk	mail@spacestudios.org.uk +44 (0)20 8525 4330

Insurance (for cyber attack)	Tokio Marine	0808 175 4376 (quote policy PI26F1130391)	UKcyberclaims@tmhcc.com
Insurance (office)	Aviva	0800 015 1498 (quote policy 97OSP3377503)	None – phone number is 24hr
Government regulator	DWP (or other govt body)	Brittany Gavit 07867 466034 brittany.gavit@education.gov.uk	SDE.SERVICEDESK@education.gov.uk 0370 267 0001
Industry support and advice	AELP	Cheryl Swales cswales@aelp.org.uk 07854497435	enquiries@aelp.org.uk 0117 986 5389
Funding submission	Cognisoft	0161 777 2901	Support website
Financial records	Xero	Xero Central	None – website is 24hr

Media

Only the media team (Tanya Murphy, Harry Simpson & Dan Williams) is permitted direct contact with the media. Anyone else contacted should direct callers or in-person media representatives to the media team.

The media team will coordinate with the media where required, according to approved guidelines to avoid adverse publicity and take advantage of opportunities for useful publicity.

Basic questions to have answers to: what happened, how did it happen, and what we are going to do about it?

Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, directors & officers' liability, general liability, cyber security protection and business interruption insurance. Details of these policies are saved within the Main Folder in SharePoint.

If insurance-related assistance is required following an emergency out of normal business hours, contact details are:

Office issue: Aviva 0800 015 1498 – policy reference 97OSP3377503

Cyber attack: Tokio Marine 0808 175 4376 or UKcyberclaims@tmhcc.com policy reference PI26F1130391

Financial & legal issues

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.

- Loss of cash
- Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post disaster
- Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

Disaster recovery plan exercises

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Jim Thomas

Jim Thomas (Sep 16, 2026 14:26:10 GMT+1)

Harry Simpson

Harry Simpson (Sep 16, 2026 12:03:01 GMT+1)

Version	Date	Author	Changes Made
1.2	Aug2026	Jim Thomas	Formatting; new details added for cyber security, terrorism, Xero & Yeti; references to ESFA updated; insurance contact details added; media section revised.

2627 GNT Continuity of Apprenticeship Training Policy (002)

Final Audit Report

2026-09-16

Created:	2026-09-16
By:	Ginger Nut Training (delivery@gingernuttraining.co.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAAQTvkep_z6bn41ttSuk74zJGqtqIHfJi

"2627 GNT Continuity of Apprenticeship Training Policy (002)" History

-  Document created by Ginger Nut Training (delivery@gingernuttraining.co.uk)
2026-09-16 - 11:01:46 AM GMT
-  Document emailed to Jim Thomas (jim.thomas@gingernut.co.uk) for signature
2026-09-16 - 11:01:52 AM GMT
-  Document emailed to harry.simpson@gingernut.co.uk for signature
2026-09-16 - 11:01:52 AM GMT
-  Email viewed by harry.simpson@gingernut.co.uk
2026-09-16 - 11:02:31 AM GMT
-  Signer harry.simpson@gingernut.co.uk entered name at signing as Harry Simpson
2026-09-16 - 11:02:59 AM GMT
-  Document e-signed by Harry Simpson (harry.simpson@gingernut.co.uk)
Signature Date: 2026-09-16 - 11:03:01 AM GMT - Time Source: server - Signature Appearance Selected: TYPE
-  Email viewed by Jim Thomas (jim.thomas@gingernut.co.uk)
2026-09-16 - 1:22:52 PM GMT
-  Document e-signed by Jim Thomas (jim.thomas@gingernut.co.uk)
Signature Date: 2026-09-16 - 1:26:10 PM GMT - Time Source: server - Signature Appearance Selected: TYPE
-  Agreement completed.
2026-09-16 - 1:26:10 PM GMT