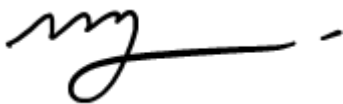




# Business Continuity and Exit Strategy Policy

<b>Prepared by</b>	<b>Authorised by</b>	
<b>Name: Martin Smith</b>	<b>Name: Warwick Nash</b> 	
<b>Date last reviewed:</b>	<b>31/07/2025</b>	
<b>Effective from:</b>	<b>01/08/2025</b>	
<b>Date of new review:</b>	<b>31/07/2026</b>	

# Scope

This policy applies to all employees of Apprentify Group Limited (the 'Organisation') and all its subsidiaries.

## Fire Procedures

Fire procedures are displayed in prominent positions, on notice boards and on our SharePoint site, around all our office locations. They include the identity of appointed Fire Marshals, emergency exits, the location of evacuation points and other procedural details. All employees must ensure that they are familiar with the emergency procedures in order to minimise the risks to life in the event of an emergency situation caused by fire.

You should familiarise yourself with all emergency escape routes, the location and types of firefighting equipment available and how to use it.

There are appointed Fire Marshals in each area of the building; it is their responsibility to instigate and coordinate the effective evacuation of the area in the event of an emergency requiring immediate evacuation. If the fire alarm sounds, you must follow their instructions. Once the building is clear a register will be taken to ensure all employees are accounted for.

It is important to practice fire procedures to ensure that they remain effective and practice evacuations will take place periodically. These drills should be treated seriously and as real fire emergencies by all employees.

If you have issues which will affect your ability to evacuate the building, you should inform the Fire Warden who will arrange for assistance. You should also inform the HR team, who may create a Personal Emergency Evacuation Plan (PEEP) for your circumstances.

If an employee discovers a fire, they should:

- raise the alarm, operate the nearest call point
- inform the responsible person of the location of the fire
- only fight a fire if you are trained or are competent to do so
- do not put yourself or others at risk by stopping to fight a fire.

If an employee hears the activation of the fire alarm, they should:

- do as instructed by Fire Marshals
- evacuate in a timely manner without delaying to retrieve personal items
- do not hinder other people's evacuation
- do not use lifts
- remain calm, walk quickly and do not run
- remain at your evacuation point until instructed otherwise

- do not re-enter the building until instructed by a Fire Marshal.

## Bomb Scare Procedures

Upon discovery of a suspicious object, package or threat of an explosive device you must be ready to assess the risks to yourself and others in the area. Following assessment of the situation you must decide on appropriate actions and act accordingly.

### Telephone Warnings

If an employee is made aware of a bomb scare by telephone, they should:

- ensure they allow the caller to deliver the full message, stay calm, do not interrupt them before engaging in conversation
- keep the caller on the phone for as long as possible whilst attracting the attention of a colleague
- inform the colleague in a discreet manner, indicating them to inform the responsible person (this would usually be the most senior person in the office at the time)
- take note of anything about the caller that may be useful to the authorities including accents, sex, any background noises and the type of language used
- the responsible person will instigate appropriate action with guidance from the emergency services.

### Suspicious Objects/Packages

If an employee is the recipient of a suspicious object or a package, they should:

- evacuate people in the immediate vicinity of the device/package and ensure that no one tampers with it
- inform the responsible person of the issue immediately.

### Evacuation Procedure

If an evacuation is deemed to be appropriate, Fire Marshals will instigate the evacuation procedure. It is important that you listen to their instruction as the evacuation plan may change depending on the nature of the threat.

Make sure that their instructions are followed as this evacuation may have been instigated by the emergency services.

# Infectious Disease Procedures

Where it is recognised by the World Health Organisation or the Government that an infectious disease creates a public health emergency, the Organisation will assess the risk posed to its workforce by the disease.

At all times, Government advice will be taken on managing our employees in relation to infection control, overseas travel, isolation periods and other relevant matters.

With regard to the severity of the risk, we may decide to:

- stagger start and finish times so that fewer people are together at once
- cancel non-essential overseas travel to affected areas across the world
- cancel non-essential training sessions
- deal with clients/customers by phone and email
- if face to face meetings must take place, ensure that facilities are suitable to minimise the spread of infection eg allowing a distance of more than one metre between participants
- deploy greater levels of flexibility including permitting employees who are usually office based to work from home.

Employees have a role to play in ensuring that the risk of infection is kept at an absolute minimum, and must themselves stick to Government guidance in relation to overseas travel etc.

## Business Continuity Management Plan (BCMP)

The following is accounted for within this plan:

- Apprentify Group Head Office and other satellite offices – Any building related Incident which affects operations from this location or the people within this location.
- Apprentify Group People – Loss of key employees who work for Apprentify Group Limited, learners, contractors and associates.
- Loss of Suppliers – People or organisations who support the Organisation's business critical operations and programmes. E.g., IT infrastructure & suppliers, gas, and electricity suppliers.
- Loss of Funding Contractor – ESFA or other funding body.

### 1. Responsibilities

In the event of an incident affecting one of the above, the following people are responsible for making sure the disaster recovery plan is put into action and monitored through to completion:

Chief Executive Officer: in the event of an incident their role is to define the risk, assess how critical it is, agree actions and release the budget to support the actions. In the event of an incident their role is to make sure the actions agreed are put into place with the support of the relevant Management Team, communicate to all staff, then oversee and monitor the actions through to completion.

## Risk Assessment

In the event of an incident occurring the following will be used to critically assess and prioritise actions:

- High – Is there a risk which affects the safety of staff, associates, and trainees and/or the immediate trading position of the Organisation
- Medium – Is there a risk to the ongoing trading position of the Organisation
- Low – there is risk, but this is a limited risk to people, resources, and trading position.

In addition to the ongoing risks outlined below, the Organisation maintains and regularly monitors a centrally-held risk register; this is owned by the Chief Finance Officer. This dynamic document records risks as they emerge and sets out risk mitigations. Below are key ongoing risks with respective continuity plans.

## 2. Business Continuity Plans for High to Medium Risk Incidents

We have identified 4 potential incidents that we would class as high or medium risk to the Organisation's premises, people and suppliers. These are:

- Loss of premises
- Loss of staff
- Loss of key supplier or supply in terms of gas/electricity/water
- Loss of IT infrastructure / systems

Detailed below are our project plans for dealing with each of the above, should the need arise.

**Loss of Office Premises:** Any building related Incident which affects operations from this location or the people within this location. (E.g., due to fire or inability to access premises).

Action to take in the event of incident:

1. CEO to access the risk and propose the actions required, i.e., length of time expected, need for equipment and if alternative location is required.
2. HR Director to contact staff members by email, Teams and/or phone to advise on loss of premises, and the plan of action.
3. CEO to contact telephone service provider so that calls are forwarded to the relevant Management Team mobile numbers.

4. All senior managers have remote access so they can work remotely. They will direct the work of their teams and communicate progress to them.
5. If site is to be unavailable for more than one day, CEO to arrange remote access, IT equipment and make sure IT provider enables all staff access to work remotely from their homes.
6. If site is to be down longer than this i.e., 1 week or more, CEO will start to arrange temporary business premises.

Recovery time from incident: Maximum of 3 hours before operational from home offices.  
Maximum of 1 week before operational from temporary office premises.

### **What need to be in place now to enable this to run smoothly should an incident occur?**

#### 1. AGL Senior Management Team

Make sure they have:

- Remote access into Apprentify servers, CRM, and Outlook
- Mobile phones and these phone numbers are on HRIS.
- Laptops or mobile devices that they can use in the event of an incident
- Access to the internet

#### 2. CRM and online systems

All staff contact details are up to date so they can be accessed from this web enabled system – this is our HRIS, BambooHR. All learner contact details are up to date so they can be accessed from this web enabled CRM system.

#### 3. Staff and Learners

Make sure all keep their CRM/HRIS and online systems up to date with current addresses and contact details.

Check who has home access to internet, computer, laptop, or mobile devices which they could use in the event of this incident occurring.

Make sure all staff have somewhere suitable at home where they could work with table, chair etc. for a short time.

Make sure all learners have alternative premises to work from or can go home.

#### 4. Equipment

Identify equipment which may be needed for staff to operate remotely. This will be done through direct communication with employees. Where the disruption is likely to last more than 3 days, equipment will be sourced and supplied to the employee where possible.

## 5. Location

Establish where might be a suitable location to approach should this incident occur. Below are alternative locations for each of our key operations spaces.

### Apprentify Limited (25, Water Lane, Wilmslow):

Apprentify has arranged an emergency location at a local apprenticeship training provider, Venn Digital, or Netcom Training.

Emergency contact at Venn Digital is Brian Whigham Managing Director [brian.whigham@venndigital.co.uk](mailto:brian.whigham@venndigital.co.uk).

Emergency contact at Netcom Training is Kevin Vashi Managing Director [kevin.vashi@netcomtraining.co.uk](mailto:kevin.vashi@netcomtraining.co.uk)

There are many available locations / rooms at Alderley Park, a local business park.

If the whole of Alderley Park is unavailable then we have also arranged temporary space at Rylands Farm 07534 794345.

If Alderley Park venues are not available then we will source temporary space at hotels and other available office spaces.

### Netcom Training Limited (ICentrum, Holt Street, Birmingham):

Bruntwood have communal space available in the ICentrum building.

In the event that the whole ICentrum building is unavailable, alternative temporary space will be arranged by using hotels or other local office space.

### The Juice Academy (Potato Warf, Manchester)

In the event that the whole building is unavailable, alternative temporary space will be arranged by using hotels or other local office space.

### Flourish Limited (111 Buckingham Palace Road, London)

The Flourish offices have communal space that can be used. There are several pay-as-you-go offices within a 20-minute walk that could be used if necessary.

### IODA Limited (Grimston Grange, Tadcaster, Yorkshire)

There are several other offices on the development that may be available with landlord consent. Alternatively, the team would need to work remotely until suitable alternative office space could be found, due to remote location.

## **Communication In an Emergency**

In the case of an emergency the employees will use the alternative routes of communication:

The appropriate all staff Teams Chat and email (for whole-staff communication).

In any case of an emergency please follow the below process:

Call the CEO on 07824 897909.

Email the relevant Director of the company.

Email the situation, location and who is involved.

Phone and email. Emergency contact details can be found below:

Name	Role	Email	Mobile
Jonathan Fitchew	CEO	Jonathan.Fitchew@Apprentify.com	07824 897909
Joe Butterfield	CFO	Joe.Butterfield@Apprentify.com	07786 692201
Sam Field	CRO	Sam.Field@Apprentify.com	07904 546 036
Martin Smith	HRD	Martin.Smith@Apprentify.com	07912 627813
Jeremy Bygrave	M&A Director	Jeremy.Bygrave@Apprentify.com	07899 891 235
Dale Walker	Director of Education	Dale.Walker@Apprentify.com	07936 361 793
SallyAnn Coleman	MD The Juice Academy	SallyAnn.Coleman@Apprentify.com	07936 361 796
Kevin Vashi	MD Netcom Training	kevin.vashi@netcomtraining.co.uk	07812332886
Sarah Skelton	MD Flourish	sarah@helloflourish.com	07813207075
Lisa Reynolds	MD IODA	lisa.reynolds@ioda.com	07584 232672

## Loss of People

Loss of key people who work for AGL due to long term illness, death, an event which means they are unable to get to their office or affects their ability longer term to do their job.

### Action to take in the event of incident:

- Determine severity of the risk and discuss options. Once actions agreed, work with AGL Management Team to agree how the work undertaken by the member of staff is to be re-allocated for an interim period and if required set up a longer-term plan of action.
- Make sure business operations can be delivered and supported, cash flow maintained, and sales performance is not adversely affected.

### Recovery time from incident

Minor incidents: Maximum of 3 hours from occurrence to work being relocated.

High risk incident: 5 days from occurrence to longer terms plan being in place.

### What needs to be in place now to enable this to run smoothly should an incident occur?

1. CEO to identify business critical staff and key activities within their roles.
2. Each critical staff member to develop a short-term recovery plan which is ready for implementation should the incident occur.



3. All communication channel through Microsoft Teams, email or telephone

### **Occurrence Affecting Current Day Delivery**

Individual's Line Manager contact learners by phone and send a follow up email to inform them of the incident and arrangements.

Where appropriate, Individual's Line Manager to contact venues/employers affected to inform them and make alternative arrangements as required.

HRD to contact next of kin, where appropriate.

### **Loss of Suppliers**

People or organisations who support the Organisation's business critical operations and programmes. E.g., IT, suppliers, Gas, Water and Electricity or Telephone suppliers.

We have identified the following as business-critical suppliers:

#### *IT suppliers*

- Bud Apprenticeships – Contact Alistair Wakefield – Apprenticeship Delivery Consultant / 07951231522 / 40 Berkeley Square, Bristol, BS8 1HP
- Magn8 – Contact
- Solaas IT – contact the helpdesk on support@solaas.rmm.service.eu or by phone on 02477102182. Alternative contact is Rene Wheeler, MD of Solaas on rene.wheeler@solaas.it

#### *Funding*

- ESFA
- West-Midlands Combined Authority
- Department for Education

From these suppliers, we have identified the following high-level risks:

- Loss of data
- Loss of supply i.e., power, phone, software, learning environment etc.
- Loss of funding

### **Loss of Data**

Action to take in the event of incident:

- Head of IT to contact the service provider to identify reason behind the loss
- Supplier to complete a data recovery from back-up system
- Supplier to arrange a replacement system or server if necessary.

Recovery time from incident: Data restored from back-up systems (disk or internet back up) within 4 hours.

### **Loss of Supply** (e.g., due to electricity supply failure. Phone line goes down)

Action to take in the event of incident:

- CFO to contact Supplier to obtain full details, find likely timescale for outage and establish risk and actions required
- CFO, supported by Management Team make sure that the plan is put into operations and all staff are communicated with

Actions implemented as per the loss of premises plan

Recovery time from incident: Maximum of 3 hours before back to operational. If a major incident Maximum of 1 week before operational to any temporary or alternative supplier/system.

### **What need to be in place now to enable this to run smoothly should an incident occur?**

- When contracting with key suppliers ensure they have strong financial position
- Ensure suppliers have their own health and safety and disaster recovery and back up process in place
- Supplier contact details held centrally on cloud storage.
- Robust back up procedures in place on/off site e.g., cloud based
- Supplier systems have daily back up of Apprentify data.

### **Loss of Funding** (e.g., inadequate or contract removed)

Action to take in the event of incident:

- CFO to contact funding body to identify the cause and timespan
- CFO to update Board members with key information and likely impact
- Team to assess the number of learners affected
- Communication to all employers and apprentices

## **Budget**

Each incident will need to be judged according to the severity of risk and action required. All action plans agreed will be costed and the CEO will define where the finances to support the implementation of the plan will be accessed from.

## **Review**

The disaster recovery process will be reviewed annually or earlier if deemed necessary.