Business Continuity Plan

COVER SHEET

Document Control

Document Title	Business Continuity Plan
Document Owner	CEO (Ritchie Mehta)
Latest Review Date	22.06.22
Review Period (annual, quarterly etc)	Every six months
Next Planned Review Date	03.01.23
Status of this version	Reviewed and updated in June 2022

Version History

Version Date	Version Number	Comments	Reviewer	Approved by	Date Approved	Approver Signature
22.06.22	1		Head of Operations (David Porter)	Managing Director (Idalina De Jesus)	22.06.22	

Location: School of Marketing Dropbox\Policies\Policies and Procedures\Business Continuity Plan

PART A - PURPOSE

- What is the purpose of the plan?

The purpose of the plan is to ensure we have the processes and measures in place to protect learners and that the business can continue to operate in the event of a significant event or disaster. The plan identifies key areas of risk and sets out an appropriate action plan for each scenario by detailing the lines of communication both internally and with learners/clients; and the recovery time objective with a high-level overview of the steps taken to mitigate and resolve likely scenarios.

- Who is it for?

This will be communicated to all employees and made available to apprenticeship employers and their learners. A copy will be made available via our website under the policies section, a hard copy will be made available in our central office in London and all senior staff are required to have a hard copy at hand so that it can be followed in the event of an IT infrastructure failure.

- When will it be used?

It will be used in the case of a significant event such as fire, flood or IT failure.

PART B - GENERAL PRINCIPLES

The Business Continuity Plan is underpinned by the below policies:

- GDPR and Data Protection/Retention Policy
- Health and Safety
- Personal Development Portfolio
- Online Safety Policy
- Subcontractor Policy

- Communications Strategy
    - Who will have overarching responsibility?
        - The Managing Director will be responsible for overseeing communications with apprenticeship employers and the Head of Operations will be responsible for overseeing communications with the learners.

    - How will notification be made
        - Dependent on the nature of the event, notifications will be made by the Programme Manager and/or Onboarding Manager. In the case of a significant event, it may be appropriate for the notifications to be made by directly by the Head of Operations and/or Managing Director.

    - What channels will be used for communications

        - Dependent on the nature of the event, notifications will be made via commonly used communication methods such as email, phone and WhatsApp cohort groups.
        - If such event involves all learners and apprenticeship employers, we would use our website to alert them of back-up measures that are being implemented (e.g. banner on home page and login page of website).

- Risk analysis
    - Risk assess each identified risk and rate them in terms of probability/impact and overall risk

All risks are rated on a scale of 1-10 (where 1 is low and 10 is high).

- Loss of key personnel resource
    - Probability: 4
    - Impact: 4
- Loss of key third party supplier
    - Probability: 4
    - Impact: 4
- Telecommunications infrastructure failure
    - Probability: 2
    - Impact: 2
- Denial of workplace access
    - Probability: 1
    - Impact: 5
- IT hardware Failure
    - Probability: 3
    - Impact: 2
- Firewall Blocking or issues
    - Probability: 4
    - Impact: 5
- Denial of service attack
    - Probability: 3
    - Impact: 5
- Server outage
    - Probability: 4
    - Impact: 4
- IT Cloud interruption
    - Probability: 3
    - Impact: 2
- Loss of data /data corruption
    - Probability: 2
    - Impact: 3
- Cyber security incident (Internal)
    - Probability: 3
    - Impact: 7

- Loss of key supplier
    - Probability: 3
    - Impact: 4
- Data breach
    - Probability: 3
    - Impact: 7
- Virus/malware/ransomware attack
    - Probability: 3
    - Impact: 7

- Key Personnel
    - Who are the names key personnel in relation to business continuity
    - Include name, role and responsibility/authority
        - Idalina De Jesus: Managing Director
        - David Porter: Head of Operations
        - Jane Richardson: Head of Quality
        - Amber Rose-Rawlings: Programme Manager
        - Bally Kaur: Onboarding Manager
        - Amy Green: Lead Development Manager

- Key Contact Details
    - Name, role, contact details – for each person
        - Idalina De Jesus: Managing Director
            - idalina@schoolofmarketing.co.uk
        - David Porter: Head of Operations
            - david@schoolofmarketing.co.uk
    - For apprenticeship provision this must include
        - Current ESFA Service centre contact information
        - ESFA contact details for the ESFA enquiry form
        - Telephone: 0370 2670001

PART C – BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN – TIME OBJECTIVES

Business Recovery Time Objectives

Action area	Recovery Time objective	Summary of impact on service
Loss of key personnel resource (sickness, adverse weather, industrial action or leave without notice)	Short-term absence (e.g. sickness): 1-2 days resource re-allocation to ensure business as usual maintained where possible (prioritising learning delivery) Recruitment of new staff – aim to recruit within 1 month and start in role within 6 weeks thereafter (dependent on notice periods and employment market)	There should be no or very limited impact on learning delivery. SoM's team of in-house tutors are equipped to support in maintaining the service and delivery at short notice in this event. To limit the impact, if a replacement tutor/key personnel cannot be found immediately, then SoM will prioritise the key personnel's tasks/learning delivery/meetings and reallocate accordingly. In certain situations, as a last resort, it may be necessary to re-arrange learning delivery sessions. SoM will communicate any rescheduled sessions to learners at the earliest opportunity via email. Note: As all learning delivery is online, the impact of rescheduling sessions is lessened (i.e. no travel time etc.). In the event that new staff need to be appointed in order to replace loss of key personnel, then temporary freelance resource (where appropriate) may be arranged to ensure

		business continuity until a permanent replacement can be found.
Loss of key third party supplier	5 working days	Limited impact – potential disruption for a small number of learners whilst a replacement is engaged, or the service provision is moved in-house.
Telecommunications infrastructure failure	1 working day	Limited/no impact expected as SoM use Microsoft Teams as the primary telecommunications method with Zoom licences in place as a suitable back-up if needed.
Denial of workplace access	1 working day	Limited to no impact on delivery to learners as all training and delivery is delivered virtually (via tutor-led sessions on MS Teams and Zoom).
IT hardware failure	2 working days	Minimal impact – replacement hardware supplied within 2 working days.
Firewall blocking or issues	3 working days	Minimal impact – learners are advised of IT requirements upon enrolment to the programme and during the induction session to ensure that any firewall blocking issues (or similar) are resolved at the outset. Usually this requires their IT department to whitelist the SoM website.
Denial of service attack	1 working day	Limited impact expected as actions taken to resolve the attack can be taken immediately (see below). SoM's in-house developer

		is equipped to resolve an event such as this in a timely manner.
Server outage	1 working day	There is a high immediate impact in the event of a server outage, however the outage should be resolved within a timely manner.

Disaster Recovery Objectives

- Details each disaster recovery area with recovery time objective and impact on service

Action area	Recovery Time objective	Summary of impact on service
IT Cloud interruption	1 working day	Minimal disruption to service as alternative software should be readily available to ensure minimal impact to delivery (if any).
Loss of data /data corruption	5 working days	All data is securely backed-up. Restoring the most recent backup available will resolve the immediate issue. The operations team will need to assess any data implications (i.e. the elapsed time between the backup and subsequent restoration).
Cyber security incident (Internal)	3 working days	Impact on service will vary depending on the nature of the cyber security incident, however the impact should be minimal to moderate (at worst) as learning delivery will be able to continue as planned – this could be via another software (e.g. Zoom / Google Hangouts) with learning resources

		sent via email if the SoM learning platform was inaccessible due to incident. If individual employee passwords/accounts are compromised due to a cyber security breach then the impact should be contained and resolved quickly without significant disruption (if any) to learners.
Loss of key supplier	5 working days	Minimal impact – see actions below for full details. In summary: it may be that internal resource is re-distributed as a temporary fix to prevent any disruption; or that a suitable alternative supplier is identified and contracted as soon as possible to minimise any disruption to learners.
Data breach	5 working days	Moderate impact – the cause / source of the breach should be investigated, identified and any necessary adjustments to procedures / training of staff made as appropriate. A *'Data Incident Report Form'* should be completed immediately following a data breach which will then be used to inform next steps. The management team will then assess the likelihood and severity of the risk to people's rights and freedoms, following the breach and inform the ICO of the personal data

		breach if the threshold has been met.
Virus/malware/ransomware attack	3 working days	Minimal impact on service as in the worst case scenario, a backup can be restored from prior to the attack.

PART D – PRIORITIES AND ACTION PLANS

As a general rule, ensuring continuity of delivery and assessment for apprentices is our top priority and this should be factored into decisions made at every stage. Once aware of the event, then the first priority should always be in identify the extent of the individuals affected, with immediate steps taken to protect against further/widening impact (e.g. securing data in the event of a breach).

Where appropriate, clear and timely communication with affected individuals (including learners, employers and staff) should be prioritised alongside the stated action plan.

Likely scenario	Loss of key personnel resource (sickness, adverse weather, industrial action or leave without notice)
Functions affected	Learning delivery
Action	All staff are required to report absence (e.g. sickness, adverse weather) at the earliest possible opportunity to enable the business sufficient time to re-allocate resources to ensure that learners experience no loss in service. Upon receipt of notification of loss of key personnel, SoM's recovery time objective is to find a replacement within 1 hour. There should be no or very limited impact on learning delivery. SoM's team of in-house tutors are equipped to support in maintaining the service and delivery at short notice in this event. To limit the impact, if a replacement tutor/key personnel cannot be found immediately, then SoM will prioritise the key personnel's tasks/learning delivery/meetings and reallocate accordingly. In certain situations, as a last resort, it may be necessary to re-arrange learning delivery sessions. SoM will communicate any rescheduled sessions to learners at the earliest opportunity via email. Note: As all learning delivery is online, the impact of rescheduling sessions is lessened (i.e. no travel time etc.).
Responsible person	Programme Manager / Managing Director
Expected implementation time	Replacement to be found within 1 hour

Likely scenario	Loss of key third party supplier
Functions affected	Learning delivery and operations
Action	When selecting suppliers, SoM have conducted research to ensure that the business is equipped with a suitable/equivalent back-up supplier. SoM's contracts with suppliers stipulate that reasonable notice should be given in the event that there will be a disruption/termination in service. Pearson TQ are SoM's only key third party supplier at this present moment in time. Pearson TQ conduct initial assessments and deliver English/Maths Functional Skills training via the BKSB platform, alongside targeted tutor support where needed. In the event that Pearson TQ were not able to fulfil their obligations, then SoM is equipped to move the performed services in-house temporarily until a strategic decision is made on the optimal long-term solution. It may be that SoM source additional internal resources (FTEs / freelancer(s)) to deliver the training; or that we instead engage a replacement supplier. Other key suppliers relating to apprenticeship delivery are EPAOs and assessment partners – suitable alternatives will be engaged, it may be necessary to seek clarity from the ESFA depending on the nature of the situation.
Responsible person	Head of Operations / Managing Director
Expected implementation time	2 days

Likely scenario	Telecommunications infrastructure failure
Functions affected	Any/all functions potentially affected
Action	SoM currently use Microsoft Teams as the primary telecommunications method. Additionally, we have Zoom licences in place as a back-up. Furthermore, in the event of disruption to both of these services (i.e. internet dependant), key personnel have work mobiles to make calls.
Responsible person	Head of Operations
Expected implementation time	0.5 days

Likely scenario	Denial of workplace access
Functions affected	N/A
Action	If a learner is unable to attend their place of work (home or office), then SoM would consult with their employer to support to sourcing and securing of an alternative location. If appropriate for the given situation, SoM would be happy for the learner to use SoM's office space in London and/or explore the possibility of arranging access to a suitable shared office space (e.g. from existing landlord or similar) near to their location. Where appropriate SoM will work with the learner and their employer to rpviode transport to the new location as appropriate
Responsible person	Programme Manager
Expected implementation time	N/A

Likely scenario	IT hardware failure
Functions affected	Any/all functions potentially affected
Action	Replacement IT hardware will be arranged and scheduled for next day delivery to personnel at their place of work.
Responsible person	Head of Operations
Expected implementation time	1 day

Likely scenario	Firewall blocking or issues – Potential for web access or developer access to the server to be impaired.
Functions affected	Learning delivery and server administrator access to the server (note: SoM operate two servers – the website server and a separate database server).
Action	The web server has UFW firewall installed to ensure connections are only allowed to certain services. In the event of an issue: inform management, identify the issue, implement solution.
Responsible person	Developer / server administrator
Expected implementation time	0.5 days

Likely scenario	Denial of service attack – A DDoS attack is an attempt to overwhelm the web server with traffic to make it slow or even unreachable.
Functions affected	Learning delivery, operations, marketing and sales.
Action	The site is monitored for uptime and alerts are sent to developer / server administrator if it becomes inaccessible. In the event of outage: inform management, identify attack by checking traffic and server logs, and formulate an appropriate mitigation plan.
Responsible person	Developer / server administrator
Expected implementation time	1 day

Likely scenario	Server outage
Functions affected	Website inaccessible – learning delivery, operations marketing and sales
Action	The site is monitored for uptime and alerts sent to developer / server administrator if it becomes inaccessible. In the event of outage: inform management, identify the cause of the problem, implement appropriate solution.
Responsible person	Developer / server administrator
Expected implementation time	1 day

Disaster recovery plan

Likely scenario	IT Cloud interruption
Functions affected	Any/all functions potentially affected
Action	Identify the issue (and potential resolution time if available) and prioritise learning delivery by seeking to locate suitable short-term alternatives to minimise disruption. Timely communication with learners and any other affected stakeholders/clients is paramount. For instance, if a cloud-based service such as Microsoft Teams was interrupted, then an alternative solution should be used instead (e.g. Zoom, Google Hangouts etc.).
Responsible person	Head of Operations
Expected implementation time	0.5 – 1 day

Likely scenario	Loss of data /data corruption
Functions affected	Website / LMS

Action	The LMS has a separate cloud hosted database server with Linode, physically located in London UK, which is automatically backed up every 24 hours with 3 backups stored in the same data center on different hardware - a daily backup, a 2-7 day old backup, and an 8-14 day old backup. In the event of data loss / corruption these backups can be restored to either the existing database server or to a newly deployed server via the Linode admin panel. In addition, a daily backup of the database itself is made and stored in data storage provided by Linode, physically located in Frankfurt, Germany. These backups may be restored to the database server by the developer / server administrator via ssh access to the server. In event of an incident: inform management, identify time / date of incident and restore most recent backup available.
Responsible person	Lead Developer / server administrator
Expected implementation time	0.5 days

Likely scenario	Cyber security incident (Internal)
Functions affected	Any/all functions potentially affected
Action	Current preventative actions that we take to guard against cyber security incidents include anti-virus software installation on work devices; tiered access to software and learner data; password manager software; guidance on appropriate password setting and use of two-factor authentication where possible. In the event of an incident: inform management, identify the cause of the problem and implement appropriate solution. It may also be necessary to update our policies/procedures or to introduce new preventative measures (e.g. additional software security). Furthermore, it may be prudent to conduct additional training with staff where necessary as a preventative measure against future cyber security incidents.
Responsible person	Head of Operations and Lead Developer
Expected implementation time	1 day

Likely scenario	Loss of key supplier
Functions affected	Any/all functions potentially affected
Action	When selecting suppliers, SoM undertake rigorous due diligence checks and ensure that the business is equipped with a

	suitable/equivalent back-up supplier. SoM's contracts with suppliers stipulate that reasonable notice should be given in the event that there will be a disruption/termination in service. In the event that a key supplier is lost at short notice, then SoM will analyse the situation and decide on an appropriate solution. For instance, it may be that internal resource is re-distributed as a temporary fix to prevent any disruption; or that a suitable alternative supplier is identified and contracted as soon as possible to minimise any disruption to learners.
Responsible person	Managing Director / CEO
Expected implementation time	2 days

Likely scenario	Data breach
Functions affected	Website / LMS
Action	Strategy / mitigation a combination of firewall and data loss / corruption points above. With the addition that in the event of a breach, once dealt with, the cause / source of the breach should be investigated, identified and any necessary adjustments to procedures / training of staff made as appropriate. A *'Data Incident Report Form'* should be completed immediately following a data breach and sent to the Managing Director and Data Protection Officer. The management team will then assess the likelihood and severity of the risk to people's rights and freedoms, following the breach and inform the ICO of the personal data breach if the threshold has been met within 72 hours of discovering the data breach. As per the ICO's personal data breach guidance documentation, the following steps should be taken immediately following a data breach within the 72 hours period. • **Find out what's happened** • **Try to contain the breach** – If we can recover the data, this should be done immediately. It's also important to consider any steps that be taken to protect those who will be most impacted. • **Assess the risk –** assess the risk of harm to those affected (e.g. learners, clients, employees, suppliers and other stakeholders) • **If necessary, act to protect those affected** • **Submit our report (if needed)**
Responsible person	Head of Operations / Managing Director

Expected implementation time	0.5 days, plus extra time for investigation into cause

Likely scenario	Virus/malware/ransomware attack
Functions affected	Any/all functions potentially affected
Action	The server is Linux – whilst not immune to attacks, it is less prone than some other operating systems. The server is set up with a firewall (see above) and is regularly updated, as is the LMS framework and any packages used. Regular backups are made as described above. No server-side antivirus is used currently. Worst case scenario, in the case of an attack, a backup is restored from prior to the attack as described above.
Responsible person	Developer / server administrator
Expected implementation time	0.5 - 1 day

Likely scenario	Managed transition to new apprenticeship training provider with clear, consistent communication maintained throughout with all parties. Note: This is in the event that SoM is unable to continue delivery and the actions would then be as noted here and in the actions section.
Functions affected	Apprenticeship Delivery Team (Operations, tutors etc.)
Action	1. SoM will work with the ESFA to identify suitable alternative training provider(s). 2. In consultation with the ESFA and other stakeholders as required, SoM will communicate the cessation of delivery with apprenticeship employers and learners, including details of the next steps to ensure that learners are able to continue their apprenticeship with a new provider; and how SoM will support with this process. Included within this, SoM will advise that any questions or concerns should be communicated and discussed within a defined time window, after which the transfer of learners to the specified new provider(s) will commence. 3. SoM will liaise with employers and learners who raise any concerns or questions on an individual basis. Depending on the nature of the concerns raised, it may be appropriate to introduce the new training provider at this point. 4. SoM will begin the process of transferring learners across to the new provider once required data agreements and ESFA approvals are secured (including DAS, ILR, 1-1 meetings, progress reviews etc.).

	5. SoM's skills coaches to meet with new provider(s) to ensure a smooth transition and to make new provider aware of any learner considerations, notes from previous progress reviews etc.
Responsible person	Managing Director / Head of Operations
Expected implementation time	1 month

Likely scenario	Ongoing access to apprentices' learning resources and portfolios maintained post-transfer to another provider
Functions affected	Operations
Action	SoM will ensure that apprentices continue to have access to learning resources and portfolios throughout the transitionary period and once the transfer to a new provider has been completed. Following discussions with the new provider, certain resources may be transferred to the new provider if applicable (with consent of the learner).
Responsible person	Head of Operations
Expected implementation time	Inline with the agreed transition timeline as discussed with the ESFA and stakeholders.