BUSINESS CONTINUITY POLICY STATEMENT

August 2019 v4

Policy

1. SCCU's policy is to maintain the continuity of its activities, systems, facilities and processes and where these are disrupted by any event, to enable it to return to 'normal' operations as soon as possible, taking fully into account the impact of any delay on SCCU's quality of service, reputation and finances.
2. This policy is intended to ensure:
    - The concept of Business continuity and our policy and approach is understood by all stakeholders.
    - Internal and external dependencies on customers, suppliers, partners and resources implications are identified.
    - SMT and Directorate plans are developed to ensure recovery continuity is assured to an acceptable level in the event of an interruption to services.
    - Plans are systematically maintained and tested.
    - A programme of training and communication is put in place.

Objectives

3. The objectives of business continuity planning are to ensure that SCCU:
    - Understand its critical activities and maintains the capability to resume operations within agreed timeframes, following the deployment of a contingency planning response.
    - Increases resilience by protecting critical assets and data (electronic and otherwise) through a co-ordinated approach to management and recovery.
    - Minimises impacts using a focused, well-managed response activity.

Scope

4. All SCCU activities wherever conducted, must comply with the requirements of this Policy.

Requirements

5. SCCU requires:
    - SMT holds the responsibility to recover generic facilities, corporately managed systems and central data security and;
    - The maintenance of a Major Incident Plan to guide the team on the recovery from major incidents. This to include call out arrangements and operational requirements and the plan must be subject to testing at least bi-annually;

- SMT and directorate is responsible for maintaining a register of all local specialist, facilities equipment and data, carrying out a business impact analysis (BIA) and setting parameters on acceptable recovery times for each. Directorate management teams are responsible for completing a Business Continuity Plan (BCP) in response to their BIA. Registers, BCP's and BIA's must be reviewed annually or following invocation of a plan so as to implement any lessons learnt. Directorate's responsible for the delivery of generic facilities which should undertake a BIA and BCP for all facilities provided through them.

6. In compiling plans due consideration must be giver to:
    - Taking all reasonable measures to prevent and avoid any disruption to normal operations.
    - Taking all reasonable measures to prevent and avoid any disruption to normal operations.
    - Consider continuity planning and resilience implications in all process, project, change and system developments.
    - Making advance arrangements for the recovery of infrastructure components (e.g. accommodation, transport, telecommunications, equipment and supplies).
    - Making advance arrangements to re-locate or re-organise operations to allow critical processes to continue.
    - Providing resilience for information systems and data, or alternative ways of working in the event of their failure. All new systems and processes to be in line with Policy.
    - Protecting staff, students, visitor and third party welfare during and following an incident.
    - Ensuring the effectiveness of plans and recovery arrangements through robust and regular testing and training.
    - Updating plans following significant changes to contingency planning requirements. Such changes may occur as part of organisational change planning and management.
    - Ensure resilience by using alternative communication channels such as phone, email and social media to contact staff, learners and stakeholders.
    - Use of cloud based business critical systems ensures resilience by limiting down time of systems and accessed anyway with WiFi or 4G tethering.

7. Individual responsibilities and actions to ensure that SCCU can continue to deliver education and training following disruptive events are described in Annex A.

Approval and review

8. Business Continuity policy approved by the SMT in January 2019.

ANNEX A

Business Continuity Responsibilities

Category	Actions	Responsibility	When
Paperwork retention	Scan existing SCCU enrolment documentation. Store in cloud and electronic media kept off site. Future enrolment documentation and portfolios to be stored electronically using OneFile.	MIS	End August 2019
Data access	MIS system is hosted off site by Provider. Staff can access PICS / OneFile / Impact / Cognassist off site for apprenticeship delivery. Enrolment packs are available on line for further enrolment	MIS	In place
Software	All software is web based and available with Wifi connection or 4G hotspot tethering. No need for connection to internal IT network.		In place
Meeting locations	Use offsite serviced offices. Existing Education partners available.	James Pease	When required
Operational locations	Work based tutors (WBT) meet learners at employer locations to provider teaching and learning and assessment delivery.	WBT	When required
Loss of transportation	Work based tutors (WBT) perform remote visits for learners using Google Hangouts / GoTo Meeting. If WiFi is not available use 4G hotspot tethering Office based staff can work off premises in line with the Working From Home policy	WBT All	When required When required
HR	HR files to be stored in Safe secured within SCCU premises	HR	June 2019
IT	IT policy for all staff when using company hardware.	James Pease	May2018
Hardware	Encryption Fire walls Permissions – safe working and access.	IT Consultant	May 2019
Telecommunications	Staff have mobile phones for communication (voice / video)	All staff	In place

Accounts - Xero	Web based accounting system available with WiFi connection or 4G hotspot tethering. Oxygen Accountantants run payroll offsite. Archiving invoices. Invoices to be scanned, stored in the cloud and on electronic media	Accounts	In place
Google platform	SCCU utilises Google platform for Office applications available with WiFi connection or 4G hotspot tethering.		In place
VOIP phones	Switchboard number can be re-directed to nominated SCCU staff member	Telecommunications provider can redirect telephones	When required
Postal re-direct	Post to be re-directed to Company Director home address until premises are available.	Accounts	When required
Working from home policy	Policy to be drafted to cover this to ensure that staff are aware of safe working off site.	SMT	May 2018
Portfolios	Portfolios that are on premises for sampling / IQA are kept in locked cabinets within storage room protected by Fire Door.		In place
Fire Drill	Procedure to be produced with other tenants of the building and tested at regular intervals.	James Pease	May 2019
Evacuation policy	Procedure to be produced with other tenants of the building and tested at regular intervals.	James Pease	May 2019
Emergency/Escalation Contact	Managing Director (SR) to contact ESFA Emergency services will contact landlord Landlord will contact Director (SR). SR to contact SMT. SMT to notify responsible staff.	SMT	
Loss of electrical supply	Premises will be available. WiFi connection not available.	All staff	In place
Loss of gas supply	Premises will be available during warm weather – may not be available during winter months	All staff	In place