Business Continuity Plan

iPET Network

Maintaining this document is the responsibility of: Sarah Mackay and Fern Gresty

This document will next be reviewed on: January 2025

The following premises are covered in this document:
iPET Network
71 Clifton Drive
Leftwich
Northwich
CW9 8BQ

Contents

Business Continuity Overview

Purpose

The purpose of this plan is to identify the potential risks to the business, prepare our business in the event of extended service outages caused by factors beyond our control, management of Third Party Suppliers and to restore services to the widest extent possible in a minimum time frame.

Outcome

The outcome of this plan is to ensure that the business can maintain a good level of service for our Training Providers and Candidates.

Plan objectives

- Serves as a guide for those implementing our business continuity plan
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.

Key employees

If a disaster occurs the members of our team tasked with enacting this plan are:
- Fern Gresty (Director)
- Sarah Mackay (Director)
- Annette Wood (General Manager)

Employees Welfare

It must be recognised that an incident that results in the enacting of this plan may also cause additional pressures for employees. Employees members need to be given clear direction about the priorities of the business. Managers must ensure that they monitor employees more closely to ensure that their welfare is maintained.

Employees should be aware of what their role is when a major disruption occurs. Clear and concise communication with employees is pivotal to having an organised response. Employees must be made aware of what communication methods are going to be used so they can find out the latest information if they are going to be working from a different location than normal.

Managers who suspect that employees have suffered undue stress or even trauma from the business disruption must consider aiding for those employees who have been affected.

Communicating with employees

In this section include details about how we would communicate with employees and Candidates. And how employees should communicate with customers, Candidates, and others, in the event of a disaster.

Communication will be created and delivered from one centralised person this being Fern Gresty, the prime communication channels will be email and telephone. Candidate information is stored on the QLMS and E-Portfolio system. Remote access is always available to these platforms and the backup is completed by a third party supplier.

All employees and Training Providers are forbidden to speak to the media and only senior members are able to

know the specifics about the incident.

Equipment

In the event of critical equipment damaged such as laptops or phones these will be replaced with immediate effect. These costs will be in the region of £1500 for replacements and will be purchased within 48 hours and operational within 72 hours of the incident however the Directors and employees remove their laptops and mobile phones on a daily basis so company wide damage by minimised and the majority of activity can still continue remotely.

Key risks and Contingency
The key risks have been prioritised as follows.

Identified Risks	Contingency
Awarding risks	
1. Certification Fraud	Most significant risk is a forged paper certificate but this will not authenticate. Should forgeries come to light, the Director will order an investigation and take such action including legal action to deter further instances. In the unlikely event that a certificate can be authenticated by someone not owning it e.g. through identity theft, the authentication of that certificate will be blocked until its true owner is traced and that ownership re-established. Any instances where significant certification fraud has occurred will be reported to the Regulators.
2. Tutor Malpractice	All centres that are delivering the iPET qualifications are risk assessed and each tutor has a Tutor Assessment of Support Rating (ASR). All tutors are vetted by iPET and provided with on-going training and support using the TNA. Most are qualified teachers or similar education professionals with industry experience or have to achieve the Level 3 AET within the first 12 months of being a Training Provider. All must sign an agreement promising to uphold standards. There is potentially sufficient professional damage to the individual from an accusation of malpractice to deter such behaviour. Should a tutor be shown to be acting unprofessionally in any way, the RO is notified, investigation commences, and their account will be suspended until it can be established that they present no risk to the qualification and system. In extreme cases legal action will be started. The regulators will be informed in any case where malpractice alleged or carried out is likely to have caused receipt of awards without proper justification. Where malpractice results in withholding awards which are due, awards will be made at no additional charge to those that have earned them.
3. Errors in assessment	The quality assurance process is designed to reduce the risk of assessment errors while keeping the cost of assessment low. In the lowest credit value qualifications, where the effect of risk is not critical, the description of levels and training are considered sufficient given the use to which these certificates will used. Feedback to tutors is designed to provide continuing professional development to make errors less likely in additional to regular standardisation and direct observation of

	the tutors. The contingencies on discovering systematic errors in a tutor's work is to inform them and require them to adjust any related work accordingly. Re-sampling will take place until it is clear that the error is eradicated. Should tutors continue to submit work that is subject to error, compulsory additional training required. In extreme cases the Tutor's account can be, and will be, blocked. Any errors that are significant and could have led to awarding of certificates that are not justified will be recorded and reported to the regulators.
4. Risk of compromising the data systems	The data system is operated using passwords and permissions. There are two sites, one that manages assessment and certificates that is deliberately separated from the one that manages general tutor / user activities. General security such as using passwords to secure written assessments, keeping software up to date, management of Third Party suppliers that are responsible for data backup and general maintenance apply. Regular backups mean that it is possible to revert to earlier versions of the data. The most likely compromise is for users to leave themselves logged in and for another person to then use that account. For example, a Tutor leaving themselves logged in and a student going to the account and awarding themselves assessment criteria. Since Tutors don't authorise awards, it would be impossible for such a failure to result in the award of a certificate without first going through the moderation procedure. It is very unlikely that a tutor would not notice a change in the patterns of assessment and these assessments have to be backed by evidence from the student. If it came to light that a student had added data and a certificate was awarded in error, the certificate will be revoked in accordance with the malpractice contingency above. Even if the student breaking into the tutors account deleted all the student information, it is not actually deleted from the system and can be reinstated. Only administrators at iPET Network can actually delete physical data and admin rights are only given to a few very users. The users of the system are monitored as those that have left iPET Network employment are locked out of the system. The data systems are hosted by a Third Party Supplier and outages are very rare. It is possible to record assessments off line in a spreadsheet and update the on-line database and so any unavailability of the site is unlikely to disrupt day to day work to any great extent. Should the system go off line through a major disaster at the Third Party, local backups are kept and so these could be used with minimal loss of data.
Business Risks	
5. Political change	Changes in government policy and DEFRA could significantly change the industry in the future. In order to mitigate this risk iPET ensures the creation of new qualifications that appeal to the market place. In terms of contingency, changes tend to happen with a year or two of notice and so the contingency is to plan to shift resources to the most viable markets in response to changes that are likely to make an existing market non-viable.
6. Bureaucratic risks	For a small Awarding Organisation, the cost of administration and dealing with several government agencies is disproportionately expensive and this raises the

	level of financial risk. iPET Network uses up to date technology to reduce the costs associated with bureaucracy. The contingency for unforeseen change is difficult except for campaigning for government agencies to use open systems and open standards and the most appropriate tools for tasks. Another strategy is for our partners / centres to be involved in trade associations such as BIGA, the trade associations are at the forefront of the changes and this information is shared to the iPET Network team. This extends the possibilities for development and language translations and reduces the risk associated with investment in innovation and development that is long term.
7. Loss of revenue	Loss of revenue is a continuing risk. Should revenue fall below a critical threshold, iPET Network would go out of business and there is nothing that could be done about it apart from a take over from a larger awarding body. However, at present development work is continuing so there is scope in the first instance to simply stop all development and review of resources in the business which may result in redundancies of employees or change of processes. That would be the first step in the contingency plan. At this point the regulators would be informed that there was a good chance that iPET Network would cease trading in the not too distant future and that eventually there would be no mechanism to maintain the database record of awarded certificates. Two options then exist. Notify Training Providers and Candidates and ensure they have printed paper manifests of their certificates and awards or arrange for the database to migrate elsewhere for at least the maintenance of authentication and printing of certificates. The former option has the disadvantage of not allowing certificates to be authenticated and lost certificates could not be re-issued. The latter option has a small cost involved but this is likely to be negligible.
8. Loss of key personnel	Each employee has a "deputy" that could take over their work at least on a maintenance level until that employee was replaced. The worst case scenario of loss of the most crucial employee would be loss of revenue to the extent that the contingency in 7 above would be invoked. However, that would take some time and so finding a replacement would be the first option.
Regulatory Risks	
9. Cost associated with compliance	Compliance with the regulatory conditions carries some overhead in providing systems to verify and respond to compliance issues. These are no more onerous than previous systems and a risk based approach provides the potential to reduce risk by prioritising resources to aspects that are the most significant. Annual review of costs within the business and speaking to new suppliers will identify the best cost effective solution for the business.
10. A. Governance	Serious problems related to governance as defined in Condition A1.2 to A1.4 are monitored through the due diligence of any personnel and declarations made to manage any adverse effects relating to the organisation and its suitability for recognition. A1.3 has been achieved and all qualifications are monitored by their uptake year on year. As a small organisation it is very unlikely that any of the causes

of non-compliance would escape the direct scrutiny of the governing body. There is no realistic chance of iPET Network being located outside the UK even if it does open subsidiary offices in other countries. (A2). It is difficult to envisage a change of control scenario where the new controller would not have a strong commitment to maintaining regulation. In this respect the risk of an adverse effect from this is very low. Conflicts of interest have been allowed for in the organisational government from the outset. The principles are well-established and there is no additional risk from the requirement to comply with the conditions. Availability of resources is fundamental to the operation of the organisation. The requirements of the conditions add no more risk to this and so the primary focus is to ensure resources are prioritised to reduce the likelihood of the most significant adverse effect. That would be to go out of business and be unable to provide continuity for verifying Candidate outcomes and qualifications. In that respect the maintenance of the systems supporting these things have been designed to be as low cost as possible and to be such that a third party with minimal training could maintain them. Risk associated with the conditions for dealing with malpractice are potentially the most significant because the degree that malpractice initiated by third parties can be controlled by iPET Network is limited. Again, the risk associated with the issue itself is more significant than the risk associated with the regulations associated with malpractice. Since regulation is itself risk based, the most significant risk to iPET Network from regulation is associated with the activities of highest risk.

11. B OFQUAL/Qualifications Wales/CCEA	There is a possible overhead in reporting requirements to OFQUAL/Qualifications Wales/CCEA but these are integrated in the general planned working practices and so the risk from the additional overhead is low. The most significant risk is in proving unlimited cooperation with OFQUAL/Qualifications Wales/CCEA in any investigation since the scope falls outside the control of iPET Network. It seems unlikely that OFQUAL/Qualifications Wales/CCEA would require such resources in such a situation that would cause iPET Network to go out of business and that is the most serious risk.
12. C Third parties	Third parties present a relatively high risk in that there are factors associated that are outside the control of the AO. Risk is minimised through a range of measures such as the completion of the Third Party Questionnaire and Management form and a clear briefing at the start of any new Third Parties providing a service. The requirements of regulation do not add significantly to that risk since, apart from reporting to and cooperating with the regulators, the rest would be done in any case. The risk in losing customers through lack of regulation is more significant.
13. D & E Qualifications	The regulatory requirements for qualifications have some administrative overhead but it is not onerous. The creation and development hold more of a resource and financial demand to ensure the design of the qualification is completed thoroughly. It is not possible to have credible qualifications without the requirements of the conditions and an estimated 95% of the work is required whether or not regulation was needed.

14. F Providing products	The requirements related to providing qualifications to purchasers are basically administrative. For this reason, the regulatory risk is low because any requirements to change anything is likely to have low bureaucratic overhead. Any Ofqual/Qualifications Wales/CCEA investigation is likely to be quickly resolved and therefor of low financial risk.
15. G Setting the assessment	Setting the assessment has risk if the regulators disagree with iPET Network's judgements related to the design and delivery of the assessments. The main issue would be to alter the design of affected assessments and this is within the existing capacity of iPET Network. There is a clear plan to make statistical and other comparisons to ensure that iPET Network assessments are in line with those of other awarding organisations in terms of their demand on candidates at a particular level.
16. H Marking	The main regulatory risk is if the regulators disagree with iPET Networks judgements related to marking and grading assessment. iPET Network would follow guidance and processes that have been developed by other AOs and so the risk of this is considered low. In a case where adjustments were needed, the expertise and capacity to do so exist and therefore the risk from regulation itself is manageable. In general, iPET Network designs assessment documents, exam papers, questions and marking schemes to be unambiguous and reviews responses from Candidates to inform refinements to make this more and more robust as the scale increases to more markers. This reduces risk from variations in marking.
17. I Appeals and certificates	The appeals procedure is well-established and in 4 years there have been a very low number of appeals. This leads us to conclude that the risk of a regulatory issue is low. Typically, certificates are issued after 8 weeks after the IQA have requested certification. The main risks associated with regulation of certificates is mainly related to administrative procedures that even if in error would be inexpensive to put right and processes and the correct naming of the certificates are in place.
18. J Definitions	We believe that we understand the definitions as presented and therefore the risk associated with definitions is low.

Third Parties Suppliers – link to the FAB website which details suppliers for AO and EPA solutions

https://awarding.org.uk/events-training-services/find-a-supplier/

Third party	Service Offered	Risk	Details	Alternative Supplier
APTECH	QLMS system	HIGH	Supplier unable to meet requirements and process of iPET Network. Supplier management process in place and the engagement report completed with any issues identified along	Quartzweb

			with the annual questionnaire completed. Additional suppliers also identified that could provide same service.	
APTECH	E-Portfolio	HIGH	Supplier unable to meet requirements and process of iPET Network. Supplier management process in place and the engagement report completed with any issues identified along with the annual questionnaire completed. Additional suppliers also identified that could provide same service.	1) Moodle 2) Onefile
ACE360	Apprenticeship LMS	HIGH	Supplier unable to meet requirements and process of iPET Network. Supplier management process in place and the engagement report completed with any issues identified along with the annual questionnaire completed. Additional suppliers also identified that could provide same service.	1) Ecordia 2) Smart Apprentices
ROGO	Apprenticeship Testing	MEDIUM	Supplier unable to meet requirements and process of iPET Network. Supplier management process in place and the engagement report completed with any issues identified along with the annual questionnaire completed. Additional	1) Certify Assessment Solutions Ltd 2) Cirrus Assessment

			suppliers also identified that could provide same service.	
Kalamazoo Direct	Certificate paper	LOW	Supplier goes out of business and can't produce certificate paper. Multiple companies that are able to print secure certificate paper and have the templates available to be sent to a new company.	1)Hague-Group 2) Secure and Confidential documents
Royal Mail	Posting of certificates	Medium	Postal strikes or issues with Training Providers receiving certificates. Ensure certificates are sent via a tracking number so iPET Network are able to track certificates that have not been received and that may need to be cancelled or recalled. This will ensure we are able to follow the correct re-printing process inline with the conditions of recognition. Other suppliers identified to for delivery options.	1) Evri 2) DPD

Scenario Examples

Below are a few scenarios that may happen within iPET Network and the solutions to resolve the risk.

Scenario 1

Premises incident - A premises incident can include flood, fire, or any other disaster that renders our office inaccessible.

Step 1: Evacuation of premises & safeguarding of employees

In office hours

Action	Details	Responsible Person(s)

1. Evacuate the building	Follow normal fire drill procedure	Fern Gresty / Sarah Mackay
2. Check evacuation is complete	Employees and visitor safety is the priority. Check everyone on-site has been evacuated	Fern Gresty / Sarah Mackay
3. Verify if incident is real	If false alarm, resume business as normal	Fern Gresty / Sarah Mackay
4. Call emergency services	999	Fern Gresty / Sarah Mackay
5. Record details of any injuries sustained in the incident	Use injury form available on employees intranet	Fern Gresty / Sarah Mackay
6. Alert employees	Alert any employees due to arrive on-site soon of the incident, and tell them to await further instructions	Fern Gresty / Sarah Mackay
7. Assess impact	Senior team meet to assess the scale of the incident & decide next steps	Fern Gresty / Sarah Mackay
8. Contact insurance company	Contact insurance company to confirm damage and process for claiming Adrian Strangwick Account Executive Web thecleargroup.com ppawinsurance.co.uk Direct 01234 361 132	Fern Gresty / Sarah Mackay

Outside office hours

Action	Details	Responsible Person(s)
1. First person on-site to notify manager	Do not enter the building	All employees
2. Call emergency services	999	All employees
3. Alert employees	Alert any employees due to arrive on-site soon of the incident, and tell them to await further instructions	All employees
4. Assess impact	Senior team meet to assess the scale of the incident & decide next steps	Fern Gresty / Sarah Mackay
5. Contact insurance company	Contact allocated insurance company Adrian Strangwick Account Executive Web thecleargroup.com ppawinsurance.co.uk Direct 01234 361 132	Fern Gresty / Sarah Mackay

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
Phones	Employees mobile phones or personal mobile phone. Contact telephone provider to forward office lines to employees mobiles Andrew Craven 0800 8778810 www.merlin-telecom.co.uk	Fern Gresty / Sarah Mackay
Internet	Employees to use home internet connections. If home connection unavailable contact local shared office providers to rent desk space or go to a local café.	Fern Gresty / Sarah Mackay
Inform insurance company	Contact details: Adrian Strangwick Account Executive Web thecleargroup.com ppawinsurance.co.uk Direct 01234 361 132	Fern Gresty / Sarah Mackay
Inform landlord	Contact details: Weavervale Housing Trust katie.steele@wvht.co.uk	Fern Gresty / Sarah Mackay
Post redirection	Form available on internet via Royal Mail	Fern Gresty / Sarah Mackay
Inform customers	If disruption is expected, inform Training Providers and customers via email	Fern Gresty / Sarah Mackay

Scenario 2

Infrastructure incident - An infrastructure incident can include the loss of computer / telephone systems, internet access, or power.

Step 1: Understand the extent of the loss

Infrastructure	Details	Responsible Person(s)
Phones	Contact phone provider to ascertain extent of outage. Contact details: BT and Andrew Craven 0800 8778810 www.merlin-telecom.co.uk	Fern Gresty / Sarah Mackay
Internet	Contact internet provider to ascertain extent of outage as above.	Fern Gresty / Sarah Mackay
Mains power	Contact power provider to ascertain extent of outage. Contact details: Better Connected Tel – 0845 217 7525 Direct Dial - 0161 710 2508	Fern Gresty / Sarah Mackay

If outage is temporary, inform employees to stay put and await further instructions. If the outage is ongoing:

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
Phones	Employees mobile phones or personal mobile phone. Contact telephone provider to forward office lines to employees mobiles Andrew Craven 0800 8778810 www.merlin-telecom.co.uk	Fern Gresty / Sarah Mackay
Internet	Employees to use home internet connections. If home connection unavailable contact local shared office providers to rent desk space or local café.	Fern Gresty / Sarah Mackay
Mains power	Employees to work from home until power is restored. If power outage is widespread and employees homes are also affected contact local shared office providers to rent desk space.	Fern Gresty / Sarah Mackay

Scenario 3

Employees incident - A employee incident can include a sudden family emergency, injury or other event which renders a key member of employees suddenly unable to work.

Step 1: Ensure no service interruption

Critical activity	Details	Responsible Person(s)
1. Identify interchangeable employees	All members of employees should have team members who can perform their roles, even if it is in a reduced capacity. Identify the relevant person and support them in carrying out business-critical activities	Fern Gresty / Sarah Mackay
2. Assess extent of loss	Identify whether the affected employees member's absence is likely to be temporary, longer-term, or permanent. Keep in mind this may be a difficult period for the employees member and / or their family.	Fern Gresty / Sarah Mackay

If the employees loss is temporary, support the member of employees who will be filling the gap until the absent member of employees returns. If the absence is long-term or permanent:

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
1. Recruit temporary or full-time replacement	Follow the standard recruitment procedure to find a full-time, part-time or fixed-term contract (as appropriate) replacement. Indeed account created to allow job roles to be uploaded quickly.	Fern Gresty / Sarah Mackay

Scenario 4

Training Provider failure to meet requirements of iPET Network standards and has received a sanction - A Training Provider fails to meet the standards or receive a sanction therefore Candidates may not be able to continue with their learning at that Training Provider.

Step 1: Ensure no service interruption

Critical activity	Details	Responsible Person(s)
1. Sanction issued with continuation of delivery of qualification to Candidate	The RO will assess the issues raised and the Governing Body will assess the sanction proposed. The RO immediately meets with the Training Provider to discuss areas of concern and how these can be rectified to ensure Candidate delivery is not affected. An action plan is put in place and increased monitoring will be carried out to ensure actions are being taken.	Responsible Officer / Sarah Mackay / Fern Gresty
2. Severe sanction issued to Training Provider resulting in stoppage of delivery	The Governing Body will assess the sanction and will immediately meet with the Training Provider to discuss areas of concern. Establish the Candidates affected and communicate with them immediately. Transfer the Candidate to the nearest Training Provider so they can continue with their learning.	Responsible Officer / Sarah Mackay / Fern Gresty

If the issues are temporary, support will be given to the Training Provider until the issues are resolved or the Candidate will be transferred to another Training Provider. For further information on sanctions please refer to the *Malpractice and Maladministration Policy including Sanctions* and *the Training Provider Agreement with Terms and Conditions.*

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
1. Transfer Candidate to another Training Provider	Ensure clear communication to the Candidates to confirm the procedure and next steps and ensure the Candidate continues with their qualification.	Responsible Officer

Scenario 5

Training Provider business failure - A Training Provider is unable to continue with their business operation due to financial reasons therefore the delivery of the qualification to Candidates is at risk.

Step 1: Ensure no service interruption

Critical activity	Details	Responsible Person(s)
1. Business failure	Director to assess the issue and immediately meet with the Training Provider to discuss areas of concern. Establish the Candidates affected and communicate with them immediately. Transfer the Candidate to the nearest Training Provider so they can continue with their learning.	Sarah Mackay / Fern Gresty
2. Outstanding payments	Director to assess the issue and immediately meet with the Training Provider to discuss areas of concern. Payment plan agreed and no further Candidates to be registered.	Sarah Mackay / Fern Gresty

If the business closing due to financial issues:

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
1. Transfer Candidate to another Training Provider	Ensure clear communication with the Candidates to confirm the procedure and next steps and ensure the Candidate continues with their qualification.	Sarah Mackay
2. Outstanding payments	Director to assess the issue and immediately meet with the Training Provider to discuss areas of concern. Payment plan agreed and no further Candidates to be registered. If payment plan fails issue to debt collectors.	Sarah Mackay / Fern Gresty

Scenario 6

Unforeseen circumstances

Step 1: Ensure no service interruption

Unforeseen circumstances may present in many forms see below for examples.

Critical activity	Details	Responsible Person(s)
1. Pandemic / Fire Flood	Due to the unforeseen event of Covid 19, it has become apparent that deadly viruses are still possible and can cause huge business interruption along with fires, flooding etc. Director to assess the issue and immediately meet with the Training Provider to discuss areas of concern. Establish the Candidates effected and communication with them immediately. iPET Network have the resources to deliver remote learning through its e-portfolio and web portal systems. Contingency policy was created within COVID to support the continued learning of the Candidates. Please note that this is reviewed on a case by case basis or requested by the Regulators.	Sarah Mackay / Fern Gresty

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
1. Transfer Candidate to another Training Provider	Ensure clear communication with the Candidates to confirm the procedure and next steps and ensure the Candidate continues with their qualification.	Sarah Mackay
2. Suspend / delay learning / assessment	Depending on the unforeseen circumstance learning / assessment may not be able to continue. Advice will be taken from the Regulators.	Sarah Mackay / Fern Gresty
3. Continued learning	Candidates have access to the E-Portfolio system to enable them to continue learning	Sarah Mackay / Fern Gresty

and tutors to remain that contact with the Candidate.

Recovery phase

The purpose of the recovery phase is to resume normal working practises for the entire organisation. Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building.

Action	Details	Responsible Person(s)
1. Agree and plan the actions required to enable recovery of normal working practices	Agreed actions will be detailed in an action plan and set against time scales with responsibility for completion clearly indicated.	Fern Gresty / Sarah Mackay
2. Respond to any long-term support needs of employees	Depending on the nature of the incident, we may need to consider providing support services.	Fern Gresty / Sarah Mackay
3. Publicise that there is now 'business as usual'	Inform Training Providers and Customers through normal channels that our business is operating as normal.	Fern Gresty / Sarah Mackay
4. Carry out a debrief of the incident and complete report to document opportunities for improvement and any lessons identified	This should be reviewed to ensure key actions resulting from the incident are implemented within designated time scales.	Fern Gresty / Sarah Mackay
5. Review this Continuity Plan in light of lessons learned from incident and the response to it	Implement recommendations for improvement and update this plan. Ensure a revised version of the plan is read by all members of employees.	Fern Gresty / Sarah Mackay

Document Control

Document Name: Business Continuity Plan
Document Number: P20

Date of Correction	Version Number	Correction Reason
	1	
	2	Update following SOC actions