Business Continuity Plan – Data Security

SELFA uses information technology to process information quickly and effectively. Our staff use email and telephone systems to communicate. Electronic data interchange (EDI) is used to transmit data including orders and payments. Laptops and wireless devices are used by our staff to create, process, manage and communicate information. This plan identifies what the Charity will do if one or more of these systems fails.

The Charity will work with Gritstone, our IT consultants, to implement technology recovery strategies to restore hardware, applications and data as quickly as possible.

Overall Responsibility

Overall responsibility for any incident and mitigations put in place sits with the Board of SELFA. They have given operational oversight to the Emergency Management Team (EMT).

This plan aligns with the Charity's Business Continuity and Disaster Plan. The EMT will comprise of:

- Chair of the Board
- Chief Officer
- Service Manager
- Senior Administrator

Gritstone, our IT consultants, will be critical to the implementation of this plan and will be contacted immediately an incident has been identified.

Systems:

Information technology systems require hardware, software, data and connectivity. Without one component of the "system", the system may not run. Therefore, our recovery strategy has been developed to anticipate the loss of one or more of the following system components:

1. Hardware (desktop and laptop computers, wireless devices and peripherals)
2. Connectivity to a service provider (fibre, cable, wireless, etc.)
3. Software applications (electronic data interchange, email, office productivity, 365 etc.)
4. Data and restoration

Scope:

The following list of IT incidents form the scope of this plan:

- Software problems and technical failures
- Unavailability of the IT network and / or systems
- Performance problems with the IT network and / or systems
- Hardware problems and failures

Asset Register

The above heading links to a register of hardware (e.g. desktops, laptops and wireless devices) and software applications.

Data Backup Strategy

No information is kept on laptop or desktop computers or wireless devices.

All of our data is cloud-based.

Our Microsoft 365 Data is backed up to the Acronis Cloud on a daily basis and these backups are encrypted.

No hardcopy vital records are kept.

Business Critical Systems:

We have considered the systems which are business critical to prioritise in this plan.

- Digital systems – 365; Salesforce (CRM); Brightpay (payroll); Liberty (accounting package); CitrusHR

All systems are Cyber Essentials compliant.

Staff have:

- Work laptops
- Personal/work mobile phones
- iPads

Business Critical Support:

We have considered the support systems:

1. Hardware – Gritstone (IT Consultants)
2. Network – Broadband/ WiFi Provider (Sky Business)
3. Digital systems – Helpdesks for each package

Loss of broadband and/or phoneline

1. In the event of the loss of access to the internet, the Senior Administrator or Service Manager will contact our broadband provider to ascertain the reason/length of the outage. All staff will be informed and encouraged to work from home where possible or use tethering to stay connected. Where this is not possible, staff will be asked to record any information in password protected documents that can be uploaded when the service resumes.
2. Where the outage will affect service delivery and/or reporting deadlines due to loss of access to data etc. the EMT will contact funders/partners involved. A course of action will be agreed with the funder(s) involved and recorded.
3. The EMT will post a notice on our website and social media to inform people how to contact the Charity where necessary.
4. The Board agree that additional costs incurred by staff in the use of mobile phones will be covered by the Charity.

System reinstated:

When broadband is reinstated:

1. The EMT will work with staff members to ascertain what information has been lost/ corrupted during the system failure.
2. This information will be documented and the EMT and staff will work to retrieve and collate the missing information as quickly as possible.
3. Where any information is irretrievable, and this could impact project's reporting to funder/ commissioning the EMT will inform these bodies as soon as practicable.
4. Reinstatement of information that could compromise service delivery to our service users will take priority.
5. Any data that has been held on any external hard drive will be transferred onto the appropriate system.
6. The EMT will update the website and social media.
7. The EMT will inform funder(s) and agree appropriate course of action in relation to reporting.

IT systems failure

A system failure can occur because of a hardware failure or a severe software issue, causing the system to freeze, reboot, or stop functioning altogether. A system failure may or may not result in an error being displayed on the screen. Computer(s) may shut off without warning and without any error message.

System failure can cause loss of hardware, software, data, or information.

The EMT will:

1. Contact Gritstone and seek advice in relation to the appropriate course of action.
2. Contact all staff impacted by the failure to make them aware of the issue and length of time to rectification.

Where the issue will cause significant interruption to provision the EMT will:

1. Contact the Board to inform them of the situation and the steps being taken to rectify.
2. Make the Board aware of potential loss of data/information relating to the Charity's operations.
3. Contact funders/commissioners/partners where the issue could impact on service delivery and/or reporting deadlines
4. Gritstone will rectify the issue that caused the failure and, where this will take a significant length of time, they will work with the EMT to establish interim measures.

Interim measures:

1. Providing password protected external hard drives to all staff members to enable them to continue to operate.
2. Reverting to paper-based systems
3. Access emails via 365 portal
4. Rental or replacement of hardware ((https://www.smart.uk.com/rental/laptop-rental/; https://devicesforteams.hardsoftcomputers.co.uk/short-term-computer-hire/).

Every effort will be made to maintain frontline delivery of services.

Where personal data could have been lost service users will be informed and this information will be re-established abiding by GDPR/ Data Protection principles.

The system failure should not have caused any breach in relation to data.

System reinstated:

If Microsoft 365 data affected, reinstate from latest backup. The EMT will then work with staff members to ascertain what information has been lost/corrupted during the system failure. This information will be documented and the EMT and staff will work to retrieve, collate the missing information as quickly as possible.

Where any information is irretrievable, and this could impact project's reporting to funder/ commissioning the EMT will inform these bodies as soon as practicable.

Reinstatement of information that could compromise service delivery to our service users will take priority.

When the system failure has been rectified then any data that has been held on any external hard drive will be transferred onto the appropriate systems.

Office unavailability

If there is a fire or flood, and office phones, computers and servers are irretrievably lost/unavailable.

Consider	Continuity plan
How will we access our systems and data e.g. • what other computers can we use • where will we work from • can we get our data back from our backups • how will we access the internet (e.g. for email and other online systems)	Liaison with Gritstone All staff working from home until new office space is sourced or current site reinstated (See BC Plan) – supplied with encrypted memory stick to store business sensitive information. Access to emails not affected as Office 365 Inform all funders/providers of issue and contingencies that have been implemented
If this happens, who needs to do what, and by when	EMT mobilised
Who needs to be told and how will we tell them	EMT – See BC Plan for details of cascading of information
What needs to be put in place so that our plan will work, who will do this and by when	Gritstone/EMT

What would happen in the event of a power outage at the Charity?

Consider	Continuity plan
How will we access our systems and data e.g. • where will we work from • what computers can we use • how will we access the internet (e.g. for email and other online systems) • For critical systems that are not online, how can we access what we need?	Staff to move to home working if in the office. All staff use laptops which can be taken home. Staff to use home broadband or tether to mobile data if this is not possible. All systems are cloud-based.
If this happens, who needs to do what, and by when	EMT informed
Who needs to be told and how will we tell them	EMT Plan
What needs to be put in place so that our plan will work, who will do this and by when	EMT

What would happen if a device failed? What would happen if a device became lost or stolen?

All staff recognise that laptops, tablets and smartphones are particularly vulnerable to becoming lost or stolen. All staff protect these items to prevent unauthorised access e.g. password protection.

Laptops are encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people) with a password to start up the device.

Consider	Continuity plan
How will we access our systems and data e.g. • what other device/s can we use • if necessary, can we get our data back from our backups • how will we prevent our data getting into the wrong hands	Staff do not use their phones to access data – they are used to access emails that would not contain PII/PID. Laptops are encrypted and all information is saved to the OneDrive and backed up remotely. Disciplinary action can be taken if staff do not abide by our Code of Conduct that identifies safe behaviour in relation to data access/storage/transfer.

If this happens, who needs to do what, and by when	If a laptop is lost or stolen then you would need to follow our data breach reporting system. The EMT and Gritstone should be informed immediately. If a phone is lost the EMT should be informed so that the phone number can be blocked. As emails are only accessed via the online portal there is limited data issue other than personal phone numbers. All clients will be informed if a phone is lost whose phone number may be compromised.
Who needs to be told and how will we tell them	EMT/ Gritstone/ clients
What needs to be put in place so that our plan will work, who will do this and by when	<u>For broken equipment:</u> Replacement can be ordered via next-day delivery and can be set up the following day. Spare phone – for use with replacement SIM. <u>For lost or stolen:</u> Our devices are difficult to get into, using strong passwords. No devices hold any PII/PID <u>Bring your own device</u> Our Bring Your Own Device Policy covers arrangements for personal devices (e.g. such as a smartphone)

What would you do if you were hacked?

Patch Management Runs Weekly for Windows, Microsoft Products and Third Party such as Chrome, Zoom & Adobe. Antivirus software helps protect our computers/laptops. A firewall blocks unauthorised access from outside of our organisation. All staff avoid unsecure or public wi-fi.

All staff are made aware of what to look out for as part of induction training and then provided with reminders at least annually and/or highlighted in other ways such as on agenda of regular meetings or in supervision.

Consider	Continuity plan
If this happens, who needs to do what, and by when	<u>Follow the breach reporting procedure:</u> For a data security breach incident report to EMT immediately and then complete appropriate incident reporting protocols. If PII/PID has been compromised, then ICO and DPST must be informed. <u>Contact Action Fraud</u>

	Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime. You can report fraud or cyber crime using their online reporting service any time of the day or night; the service enables you to both report a fraud and find help and support. You can talk to their fraud and cybercrime specialists by calling 0300 123 2040 Change passwords Passwords would need to be changed immediately. Restore backups If necessary, as a way of retrieving information
Who needs to be told and how will we tell them	EMT/Gritstone/colleagues affected Clients whose PII/PID has been directly compromised informed by their worker or by the EMT.
What needs to be put in place so that our plan will work, who will do this and by when	NA
What prevention measures do we have in place in terms of our technical approaches?	Keep operating systems and software up to date for all devices Use anti-virus software on computers and laptops Implement a firewall for our offices' internet connections Avoid unsecure or public Wi-Fi
What prevention measures do we have in place in terms of staff training?	Staff awareness training – as part of induction Retraining annually

What would happen if Salesforce went down:

Consider	Continuity plan
What critical aspects of our business will be affected?	All staff would be unable to extract or input any information relating to service users.
How will we access the information that we need?	We would put a temporary paper or spreadsheet system in place to maintain records of interaction with service users (password protected)
If this happens, who needs to do what, and by when	Contact Salesforce

Who needs to be told and how will we tell them	Staff Team
What needs to be put in place so that our plan will work, who will do this and by when	All staff need to be aware of the action to take should Salesforce go down.

Change Record

Date of change:	Changed by:	Comments
21/09/2023	Rosie Hall	Policy created