Advanced IT Services

ICT & Communications Services Disaster & Recovery Plan

with

George Spencer Academy

www.aitn.co.uk

Advanced IT Services - Arthur Mee Road, Stapleford, Nottingham. NG9 7EW

Email: info@advanceditservices.co.uk **Head Office:** 0115 9170197

Contents

Contents 2
Introduction 3
Plan Assumptions 3
ICT Continuity Plan 4
Academy ICT Requirements 5
Responsibilities 5
Principle Recovery and Invocation Procedures 6
Plan of Action 7
Revision Plan 8

Introduction

Due to the nature of the service provided by the Academy and the dependency upon the main computer server systems, loss of these facilities would curtail the Academy's activity to such an extent that administration or teaching could not continue in their current form unless an alternative location running all critical services was found quickly.

Likely causes

- Fire (possibly just local to server facilities)
- Flooding
- Sabotage
- Theft
- Loss of Facility support services
- Sustained power loss
- Sustained telecommunication failure
- Software malfunction

IT and Communications Services Department of George Spencer Academy seeks to ensure that the Academy education and administration processes are protected from disruption and that the Academy disaster team is able to respond positively and effectively when disruption occurs.

This ICT continuity and recovery plan ensures that the required information and communications technology and services are resilient and can be recovered to predetermined levels within timescales required by and agreed with the Principal of the Academy.

The approach taken in delivering the Disaster Recovery Plan is as a priority to ensure appropriate the Academy staff resume access to key normal processes supported by IT systems. This will help deliver core services to staff and pupils that will enable full service levels to be resumed.

Plan Assumptions

- The plan is designed to recover from the "worst case" destruction of the George Spencer Academy's operating environment. The worst case includes any non-data processing function that may be in close proximity to the data centre or workstations.

- The "worst case" destruction assumes the loss of the total facility, supporting infrastructures (Power grids, Network fibre links, external communication, data and switching).

- Although the plan is designed for worst case, inherent in the plan strategy is the ability to recover up to the most minor interruption, which is perhaps a more likely situation.

- The plan is based upon a sufficient number of staff not being incapacitated to implement and affect recovery. Therefore, the level of detail of the plan is written to a staff experienced in the operation of George Spencer's computer services. Any development, testing and implementation of new technologies and applications are

suspended so that all resources are available to recover existing critical production processing.

- Off-site inventory and equipment acquired through vendors is considered to be the only resource with which to recover computer processing. Items at the original site are not expected to be salvageable and used for recovery. For worst case this would include items stored in any on-site security location.

- An alternate on-site location in which to establish recovery of ICT System processes is necessary. Time frame requirements to recover computer processing are significantly less than estimated times to repair/reconstruct a data centre on an emergency basis.

ICT Continuity Plan

The scope of the ICT Continuity Plan covers:

a) IT services
   - Servers associated with System control and facilities
   - Servers associated with student and staff contact information (SIMS).
   - Servers associated with Academy finance systems and data.
   - Servers associated with student and staff saved data.

b) Telecoms services.
   - All corporate telephone extensions
   - All mobile phones

but currently excludes

c) IT services
   - Equipment associated with CCTV.
   - Equipment associated with electronic site security.

d) Telecoms services
   - Internet Connection.
   - Non-George Spencer infrastructure including power grids and telephone switching

The person in charge of the adherence to the ICT continuity plan is Systems Manager and he is responsible for ensuring that the plan is continued to be carried out and that any changes in the ICT strategy are implemented within ICT continuity plan.

The plan is to be reviewed each year including the scope of service covered as part of a continuous improvement strategy. It will also be reviewed for its integration into the wider Academy Disaster Plan and amended accordingly for any changes in activity or identified risk.

Academy ICT Requirements

The ICT services to the Academy have been identified

Priority	Service Name	Service/Product Supported	Effect
High	*SIMS*	*Personal contact data for all staff and pupils*	*Lack of parental contact*
Medium	*Sage*	*Financial Systems*	*Could impede recovery funding*
High	*eMail*	*Operational contact with external agencies*	*Major communications tool*
High	*File Servers supporting all student and staff data*	*Staff and pupil operational data*	*Required to restore normality in teaching and learning*
Medium	*File Servers supporting general business applications*	*Word processing, spread sheet and database programs*	*Required to restore normality in teaching and learning*
Low	*Web*	*Internet Access*	*Variable*
Medium	*Wireless Networks*	*Laptop support*	*Lack of workstation availability*

The Disaster Recovery Plan is structured to ensure that the most important or time critical Academy processes are tackled first, with other processes being brought back as time permits. In general, the following priority list is correct:

- Administration Services
- Finance Services
- Data services
- General Applications
- Web

Responsibilities The ICT services team is responsible for all computer networking and communications. In the event of the recovery plan being enforced the ICT team are responsible for bringing computer networking and communications back online.

The ICT Services Team are also responsible for the following:

- Arranging new local and wide area data communications facilities and a communications network, which links the standby location to the critical users
- Installing a minimum voice network to enable identified critical telephone users to link to the public network.
- Prepare and install all new equipment as required to bring network and communications back online.

Principle Recovery and Invocation Procedures

- Evaluate the extent of damage to the voice and data network and discuss alternate communications arrangements with telecoms service providers.
- A Telephone divert service should be activated as appropriate if phones of building effected
- Procure and install all new hardware as necessary.
- Establish the network at the standby locations in order to bring up the required operations.
- Define the priorities for restoring the network in the user areas.
- Advise staff of how to access IT services and time of last snapshot of data and if necessary with newly issued access credentials.
- Order the voice/data communications and equipment as required.
- Supervise the line and equipment installation for the new network.
- Providing necessary network documentation.
- Provide ongoing support of the networks at the standby location.
- Certain staff to work from home using internet broadband or mobile internet
- Re-establish the networks at the primary site when the post disaster restoration is complete.
- Certain staff permitted to work from home using internet broadband or mobile internet
- Advise staff of how to access IT services and time of last snapshot of data with newly issued access credentials
- Service Delivery team would salvage any equipment which may still be of use.
- Prepare/update and Execute plan for migration back to original newly repaired/prepared Datacentre Facility
- Detail list of ‘Lessons’ learned to improve Plan

Plan of Action

Immediate

Alert and mobilize all team members.

Within Three Hours

- Contact relevant staff with lay systems responsibilities (SIMS, Finance etc.); inform them of the scenario and the actions being taken.
- Apprise ICT Services staff of any temporary instructions.
- Start the download and checking of all data backups.
- Begin compiling an inventory of surviving communications equipment (voice/data) and that needing to be acquired.
- Ensure that all relevant documentation is at hand or retrieved from the off-site storage location, for the reinstatement of the network.
- Liaise with the whole school team leader as to the status of communications and assist with acquiring replacement equipment if required.
- Provide further information to enable the Systems team leader to keep users informed of current position if required.

Within Twenty Four Hours

- Define the priorities for restoring the network on a gradual basis in order to provide a minimum initial requirement for normal operations.
- Liaise with suppliers of communications or systems equipment to ensure prompt delivery, if required.
- Ensure that the reinstated communications and systems network is operable and tested.
- Provide on-going support for the network and carry out any re configuration of the reinstated network that may be necessary.
- Install all the necessary replacement hardware.
- Re instate the downloaded backups onto the new hardware using virtualisation.

On-Going

- Monitor the network's performance.
- Monitor and deal with users' requests in the light of the restricted network.

- Prepare an inventory of all communications equipment requiring replacement in order for the original computer processing environment to be re utilised.
- Order replacement equipment as required in conjunction with the Principal and Business Manager (for expenditure approval).

Revision Plan

The Disaster Recovery Plan (DRP) and the risk assessment will be formally reviewed on a 6 monthly basis, timed to incorporate lessons learned from the most recent test. In response to this, the plan will be re-evaluated, and revised versions of it distributed to all employees with explicit roles and responsibilities in a DR scenario.