IT Disaster Recovery Plan

1. Version control

Date	Version	Revision	Owner
08/03/18	1.0	New Policy	Future Generation Trust Policy Team
07/03/19	2.0	Amendment to Policy	Future Generation Trust Policy Team

2. Contents

3. Introduction

The purpose of this document is to set in place strategies to ensure the secure backup and recovery of important data that is stored on the Trust and individual academy administration and curriculum networks. The data to backup includes Trust documents, management data files, administration network user documents, teaching staff documents and pupil documents.

Future Generation Trust's (FGT) data is currently hosted on the network at the site of its registered office; St John's Primary Academy.

The strategies in place will be robust enough to ensure the recovery of data in any circumstances. Identified risks are:

- Fire or flood
- Electrical failure or surge
- Catastrophic hardware (including portable media) or software failure
- Virus or hacker attack
- Accidental damage to hardware
- Theft of hardware
- Accidental file deletion

Data can be destroyed by system malfunction or accidental or intentional means. Regular backups will allow data to be readily recovered as necessary. Enabling shadow copies on the network shares gives increased flexibility with work accidentally deleted, or purposefully deleted. The ongoing availability of important data is critical to the operation of the Trust and individual academies. In order to minimise any potential loss or corruption of this data, individuals responsible for providing and operating administrative applications need to ensure that data is routinely backed up by establishing and following an appropriate system backup procedure.

3.1 Statement of Authority and Scope

This plan is intended to detail the accepted good practice in the backing up and restoring of data on the networked computer system.

The Learning Technologies Manager and managed service provides the framework, design and implementation of backup strategies to be employed at the central hub based at St John's Primary Academy and at individual academies within the Trust. The Learning Technologies Manager, the managed service and Headteacher of each Academy are then responsible for the operation of these strategies, with the full support of the FGT Senior Leadership Team and their Local Governing Body.

3.2 Data to be backed up

- All FGT data
- Administration document files including Outlook
- Curriculum network user files
- Staff document files
- Pupil document files

3.3 Backup Hardware

All individual academies will have a documented procedure in place that outlines a strategic, timetabled backup process.

Similarly, there will be a documented procedure in place for the daily backup of FGT data.

3.4 Plan Assumptions

- The plan is designed to recover from the “worst case” destruction of the Trust’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 the Trust’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.

4. 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.
- Servers associated with Academy finance systems and data.
- Servers associated with student and staff saved data.

b) Telecoms services.
- All corporate telephone extensions

but currently excludes;

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

d) Telecoms services
- Internet Connection.
- Infrastructure including power grids and telephone switching

The person in charge of the adherence to the ICT Continuity Plan is the Learning Technologies Manager and they are 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.

5. Academy ICT Requirements

The following ICT services to the Trust have been identified

Priority	Service Name	Service/Product Supported	Effect
High	*SIMS/ScholarPack*	*Personal contact data for all staff and pupils*	*Lack of parental contact*
Medium	*PSF Financials*	*Financial Systems*	*Could impede recovery funding*
Low	*eMail*	*Operational contact with external agencies. Cloud based so minimal disruption (O365).*	*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*	*Chromebooks/Laptops*	*Lack of workstation availability*

The I.T. Disaster Recovery Plan is structured to ensure that the most important or time critical Trust and 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

5.1 Responsibilities

The Learning Technologies Manager and managed service are 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.

6. 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.
- Order the voice/data communications and equipment as required.
- Supervise the line and equipment installation for the new network.
- Provide 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 site when the post disaster restoration is complete.
- 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

7. Plan of Action

7.1 Immediate

Alert and mobilise all team members including managed service.

7.2 Within Three Hours

- Contact relevant staff with lay systems responsibilities (SIMS/ScholarPack, Finance etc.); inform them of the scenario and the actions being taken.
- Apprise managed service 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 Headteacher as to the status of communications and assist with acquiring replacement equipment if required.
- Provide further information to enable the Headteacher to keep users informed of current position if required.

7.3 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.

7.4 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 Headteacher and Head of Finance and HR. (for expenditure approval).

8. Disaster Recovery

The network and the server are covered by a managed services contract with Entrust IT Services Division. The helpline number is 0333 300 1900 or LT@entrust-ed.co.uk They should be contacted immediately in the event of a server breakdown.

All other PCs, servers and laptops are covered to an extent with Entrust I.T. The Learning Technologies manager will attempt recovery of lost data using disaster recovery software, from up to date backups where available.

9. Monitoring and Review

This 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 to ensure that the plan incorporates the requirements of any new Academy joining the Trust and to ensure its integration into the wider Business Continuity Plan. The plan will be amended accordingly to accommodate any changes in activity or newly identified risk.

Policy adopted on: **18 March 2019**

Review Date: **March 2020**

Signed: **Fliss Dale** **Designation:** **Chair of Trust Board**