Newfield Central School District

Technology
Disaster Recovery Plan

Office of Technology & Professional Development

This plan is intended to create a framework for responding to various incidents that impact the continuity of operations for the district information technology infrastructure.

Revision History

Revision	Date	Name	Description
New	October 2018	C Griggs, R Fisher, C Gaspari	Initial Creation/documentation

Information Technology Statement of Intent

This document delineates our procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our school community, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Goals

- The district shall develop a comprehensive IT disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the district recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and district business operations.

Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective disaster recovery capabilities as applicable

Key Personnel Contact Info (attempt to call in order listed)

Name, Title	Contact Option	Contact Number
Dr. Cheryl Thomas	Work	607-564-9955 X4140
Superintendent	Mobile	[redacted]
	Email Address	
	Alternate Email	
Cathy Griggs	Work	607-564-9955 X5124
Director of Technology & PD	Mobile	[redacted]
	Home	
	Email Address	
	Alternate Email	
Debra Eichholtz	Work	607-564-9955 X4140
School Business Administrator	Mobile	[redacted]
	Email Address	
	Alternate Email	
Robert Fisher	Work	607-564-9955 X5030
Network Specialist	Mobile	[redacted]
	Home	
	Email Address	
	Alternate Email	
Christopher Gaspari	Work	607-564-9955 X4105
Microcomputer Specialist	Mobile	[redacted]
	Email Address	
BOCES RIC	Helpdesk	315-433-8345
	Email Address	helpdesk@cnyric.org
	Joe Scott	[redacted]
	Jason Graham	
Steve Yaple	Work	607-564-9955 X4129
Director of Facilities	Mobile	[redacted]
	Email Address	

External Contacts (call based on nature of incident)

Name, Title	Contact Option	Contact Number
Power Company: NYSEG	Customer Service	800-572-1111; 800-600-2275
	Report Outages	800-572-1131
	Email Address	Email form at nyseg.com
T**elecom: First Light (formerly FLTG)**	**CONTACT CNYRIC FIRST**	
	Equipment Repair Service	833-484-0404
	Email Address	Repair@firstlight.net
	Sales Support & Billing	888-832-4976
	Email Address	Customerservice@firstlight.net
Telecom: Verizon	CONTACT CNYRIC FIRST	
	Email Address	
	Sales Support & Billing	888-743-7211
	Email Address	
Insurance : Utica National	Local Agent: Frank Smith	607-257-6035 X40931
	Work	800-598-8422
	Email Address	Email form at uticanational.com
Site Security: Day Automation		
	Work	800-836-0969
	Email Address	Servicedesk@dayautomation.com
HVAC: Johnson Controls	Work	585-924-9346
Printers: Eastern Managed Print Network	Service	888-652-6902
	Supplies	888-652-6904

Table of Contents:

1. Plan Overview
2. Emergency Response
3. Media
4. Insurance
5. Financial/Legal Issues
6. IT Disaster Recovery Plan Exercises

1 Plan Overview

1.1 Plan Updating

It is necessary for the Instructional Technology Disaster Recovery Plan (IT DRP) updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments will be made to the procedures.

1.2 Plan Documentation Storage

Copies of this Plan and hard copies will be stored in secure locations to be defined by the district. Each member of administration will be issued an electronic copy and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

1.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Utilize disk and tape backups. Relaunch servers using Veeam (virtual server) backup.
Tech Support - Hardware	Hardware support contracts—Dell & CISCO for the network.
Tech Support - Software	CNYRIC for administrative software (Wincap) and student information system (School Tool). Microsoft for Office 365.
Facilities Management	Metasys—HVAC controls (Johnson Controls backup and relaunch), Continuum—Access controls (through NCSD tape backup & Day Automation), RTU—Intrusion Alarm System (Day Automation), Fire Alarm Service Technology (offsite)—fire alarms
Email	Email is through Microsoft Office 365 and is cloud based. In an emergency we would use the cloud solution exclusively.
Purchasing/Finance/Human Resources	Wincap is maintained and hosted at CNYRIC. Backup services are from CNYRIC.
Web Site	Maintained and hosted at CNYRIC.

1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined.

The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	5	2	All critical equipment is located in the Elementary server room. Switches are throughout the district.
Tornado	5	1	Tape backups are stored in different building than servers. Backup to disk is housed in the server room. Rebuild from what would be available. Utilize the cloud-based services as available.
Electrical Surges, Loss of Power, and Lightning	3	2-5	Servers and switches are connected to UPS units to minimize electrical surge damage.
Fire	3	2-3	Tape backups are stored in different building than servers. Backup to disk is housed in the server room. Rebuild from what would be available. Utilize the cloud-based services as available. Replace hardware as needed.
Loss of communications, network services	1	3	Usually temporary. CNYRIC as ISP contacted to help rectify issues.

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

2 Emergency Response

2.1 Alert, escalation and plan invocation

2.1.1 Plan Triggering Events

Key trigger issues that would lead to activation of the Technology Disaster Recovery Plan are:

- Total loss of all communications
- Total loss of power

- Water damage
- Loss of the building, due to fire, flood, etc.

2.1.2 Assembly Points

Where the premises need to be evacuated, the Technology Disaster Recovery Plan invocation plan refers to the building level Emergency Plan.

2.1.3 Activation of Emergency Response Team

When an incident occurs a modified district level crisis team will be established, to include the Director of Technology & Professional Development, Network Specialist, Microcomputer Specialist, Superintendent, Director of Facilities, and any other necessary individuals. This team will then decide the extent to which the Technology Disaster Response Plan must be invoked. The response team will determine the following:

- Assess the extent of the disaster and its impact on the district technology profile
- Decide which elements of the Technology Disaster Plan should be activated;
- Establish and manage Technology Disaster Recovery Team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

2.2 Disaster Recovery Team

The team will be contacted and assembled by the Director of Technology & Professional Development, Network Specialist, Director of Facilities, and the Superintendent and/or their designee.

The team's responsibilities include:

- Establish facilities for an emergency level of service;
- Coordinate activities with disaster recovery team, first responders, etc.
- Restore key services;
- Recover to business as usual.

2.3 Emergency Alert, Escalation and Technology Disaster Recovery Plan Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The Technology Disaster and Recovery Plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the school returns to normal operating mode.

2.3.1 Emergency Alert

The person discovering the IT incident calls the Director of Technology and Professional Development and Network Specialist. The Director of Technology will notify the Superintendent, Director of Facilities, and CNYRIC if necessary.

One of the tasks during the early stages of the emergency is to notify the Technology Disaster Recovery Team that an emergency has occurred. The notification may request TDRP members to assemble at the site of the problem.

3 Media

3.1 Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with communications protocols outlined in the Districtwide and Building Level Safety Plans.

3.2 Rules for Dealing with Media

Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media contact.

4 Insurance

As part of the company's disaster recovery and school district continuity strategies, a number of insurance policies have been put into place with Utica National Insurance.

5 Financial and Legal Issues

5.1 Financial Assessment

The School Business Administrator shall prepare an initial assessment of the impact of the incident on the financial affairs of the district. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

5.2 Financial Requirements

The immediate financial needs of the district must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of district credit cards to pay for supplies and services required post- disaster

5.3 Legal Actions

The Superintendent with the School Business Administrator will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the District.

6 DRP Exercising

Disaster recovery plan exercises are an important part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that teams are familiar with their assignments and, more importantly, are confident in their capabilities.