APPENDIX 7

ICT Disaster Recovery Plan

This policy was approved and ratified by the Governing Body of

Cox Green School

on 20th October 2015

Signed: ____

Chair of Governors

Date: ____

Version	Authorisation	Approval Date	Effective Date	Next Review
1	Full Governing Body	28/02/12	28/02/12	Sept 2012
1.1	Full Governing Body	09/10/12	09/10/12	Sept 2013
1.2	Full Governing Body	15/10/13	15/10/13	Sept 2015
1.3	Full Governing Body	20/10/15	20/10/15	Sept 2017

Index of Document

Purpose and Scope

Introduction

Cox Green School (CGS) has a highly computerised operational environment. This includes the use of servers, Laptops, PCs and peripherals across the whole site. A school-wide network ties these various systems together and provides communications to other computer networks. In addition, the operation of the School network provides a vital support component of the School system.

The reliability of computers and computer-based systems has increased dramatically in the past few years. Computer failures that do occur can normally be diagnosed and repaired promptly using both local and remote diagnostic facilities. The school servers contain redundant parts, which improve their reliability and provide continual operation when some failures occur.

The infrastructure design has resilience, with built-in network redundancy, enhancing our ability to cope with a major disaster. Failure of part of the network would not necessarily disable the remainder of the site.

For the most part, the major problems that can cause a computing system to be inoperable for a length of time result from environmental problems related to the computing systems. The various situations or incidents that can disable, partially or completely, or impair support of CGS's computing facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require special funding from the School in order to allow the affected systems to be repaired or replaced. This report assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery.

Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the central site or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting CGS's computer network. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical running of the School, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the computing support given to CGS clients from academic and administrative systems within the remit of the ICT Network Team. Each department at CGS should develop their own internal plans to deal with manual operations should computer and/or network services be disrupted.

All major servers that are vital for the daily operation of the School are maintained under a next business day or 4 hour mission critical warranty. This ensures that routine maintenance problems will be addressed in a timely way with adequate resources. This support contract provides telephone support, and full hardware replacement on site.

Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. The schools senior leadership team will make any special decisions for situations not covered in this plan needed at the time of an incident.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first one on site following an incident will contact the IT Systems Manager for a determination of the need to declare an incident. The Head Teacher will also be notified.

The school IT Systems Manager will assume immediate responsibility. The first responsibility will be to see that people are evacuated if needed. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured. The CGS Administration Office and Headteacher will be notified. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., **but** evacuation is the highest priority.

Once an incident which is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper School authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable computer and/or telephone support to the School has been re-established.

Incidents Requiring Action

The ICT disaster recovery plan for CGS will be invoked under one of the following circumstances:

1. An incident which has disabled or will disable, partially or completely, the School Network facilities for a period of 24 hours.

2. An incident which has impaired the use of computers and networks managed by IT Support Team due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all academic and administrative systems which the IT Support Team manages.

3. An incident, which was caused by problems with computers and/or networks, managed by the IT Support Team and has resulted in the injury of one or more persons at CGS.

4. An incident that involves virus attack, or unauthorized intrusion onto the schools network, endangering the security and integrity of the schools Administration data.

Contingencies

General situations that can destroy or interrupt the computer network usually occur under the following major categories:

- Power/Air Conditioning Interruption
- Fire
- Water
- Weather and Natural Phenomenon
- Sabotage, virus, unauthorized intrusion onto the network.

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- Partial recovery - operating in alternate client areas within the School.
- Full recovery - operating in all client areas, possibly with a degraded level of service for a period of time.

Physical Safeguards

Lockable doors protect the CGS server room. The IT Support Team have access to the keys. The room is air conditioned and protected by the school fire alarms. The server room windows are covered with iron bars. The schools CCTV system also covers the server room area. The server room door has 2 deadlocks with different keys, this door has limited key holders for security.

Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve CGS's Networking facilities. Some minor hardware problems do not disrupt service; maintenance is scheduled when convenient for these problems. Most hardware problems disrupting the total operation of the computers are fixed within a few hours.

Major networking problems

Experiences at CGS with Dell replacing failed hard drives in one of the main ~~domain~~ servers, enabling CGS to have no down time. Cabling attached to catenaries connecting the school site together failed under extreme cold. We asked a fiber optic cabling specialist to come and replace with higher rated cabling for extreme heat/cold weather.

Major telephone problems

Problems regarding outside telephone lines are the responsibility of the telecoms infrastructure company. The responsibility for the upkeep and maintenance of the internal telephone system is the schools telephone contract provider.

Environmental problems (air conditioning, electrical, fire)

An external maintenance company periodically services the air conditioning units, any faults are reported to the Facilities team, and repaired by the maintenance company.

Electrical

In the event of an electrical outage, all servers and other critical equipment are protected from damage by Uninterruptible Power Supplies (UPSs). These units will maintain electrical service to our servers long enough for them to be shut down gracefully. Once electrical power is restored the servers will remain “powered down” until the UPSs are recharged a sufficient amount to ensure the servers could be gracefully shut down in the event of a second power failure.

Fire

All server rooms are equipped with fire extinguishers, which will adequately provide manual fire suppression to the equipment from fires in the room itself. If a fire starts, the fire extinguishers should limit damage to the affected piece of equipment and the possibility of damage to equipment in the immediate vicinity. The server room is also fitted with a smoke detector that links to the main school system.

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all our hardware. Our critical data is backed up daily, a copy which is stored outside of our main server room. Each weekend a simple backup of key systems is taken off site on an encrypted device by the IT Systems Manager. A full backup of key systems is taken off site each half term by the IT Systems Manager on an encrypted device. This sufficiently protects the school from a full site disaster.

Insurance Considerations

All major hardware is covered under CGS's standard Property insurance for the School.

ICT Recovery Team

ICT Disaster/Recovery Team Headquarters

1. If the Server room is usable, the recovery team will meet in the Server room.
2. If the Server room is not usable, the team will meet in the IT Support Office, Main School.
3. If the Main School is not usable, the team will liaise by mobile phone.
4. If none of the School facilities are usable, it is presumed that the disaster is of such proportions that recovery of computer support will take a lesser priority. The ICT Disaster Recovery coordinator will make appropriate arrangements.

ICT Disaster Recovery Coordinator

The IT Systems Manager will serve as ICT Disaster Recovery Coordinator. The major responsibilities include:

- Determining the extent and seriousness of the disaster, notifying the Head Teacher & Business Manager immediately and keeping them informed of the activities and recovery progress.
- Invoking the ICT Disaster Recovery Plan after approval.
- Supervising the recovery activities.

- Coordinating with the Head Teacher & Business Manager on priorities for clients while going from partial to full recovery.
- The IT Systems Manager and IT Support team will keep staff and students informed of the recovery activities.

The IT Systems Manager will be responsible for:

- Coordinating hardware and software replacement with the academic hardware and software vendors.
- Coordinating the activities of moving backup media and materials from the off-site backup files and using these for recovery when needed.
- Keeping the Head Teacher & Business Manager, or in their absence, the Deputy Head Teacher, informed of the extent of damage and recovery procedures being implemented.
- Coordinating recovery with departments, those using the academic computers and/or those Administration functions.
- Coordinating appropriate computer and communications recovery.

Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site backup device contains adequate and timely server backup's and documentation for applications systems, operating systems, support packages, and operating procedures.

As part of the schools Disaster Recovery Plan it is essential that key data can be accessed under any circumstance within a suitable time period.

General Procedures

Responsibilities have been given for ensuring each of the following actions have been taken and that any updating needed is continued.
Maintaining and updating the ICT disaster recovery plan.

- Ensuring that all IT Support team members are aware of their responsibilities in case of a disaster.
- Ensuring that the periodic scheduled backup plan is being followed.
- Maintaining and periodically updating ICT disaster recovery materials, specifically documentation and systems information, stored in the school safe on an encrypted device and on off-site encrypted backup device.
- Maintaining a current status of equipment.

- Ensuring that UPS systems are functioning properly and that they are being checked periodically.
- Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.
- Ensuring that proper temperatures are maintained in server areas.

Software Safeguards

Administrative software and data are secured by incremental backup's each weekday evening. The full copies of software are backed up weekly or termly depending on changes.

Recovery Procedures

This portion of the disaster/recovery plan will be set into motion when an incident has occurred, and damage is such that operations can be restored, but only in a degraded mode at the central site in a reasonable time. It is assumed a disaster has occurred and the administrative recovery plan is to be put in effect. This decision will be made by the Head teacher/Deputy Head & Business Manager upon advice from the IT Systems Manager.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
- Rush order any supplies, forms, or media that may be needed.

In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternative site:

- Notify Headteacher that an alternative site will be needed or alternative facilities.
- Coordinate moving of equipment and IT support team to the alternative site.
- Bring the recovery materials from the backup storage to the alternative site.

- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Determine the priorities of the client software that need to be available and load these packages in order. These priorities often are a factor of the time of the month and academic year when the disaster occurs.
- Set up operations in the alternative site.
- Coordinate client activities to ensure the most critical jobs are being supported as needed.
- As production begins, ensure that periodic backup procedures are being followed and encrypted backup devices are taken off-site as per the schools backup plan Work out plans to ensure all critical support will be phased in.
- Keep administration and users informed of the status, progress, and problems.
- Coordinate the longer range plans with the administration, the site officials, and staff for time of continuing support and ultimately restoring the overall system

Degraded Operations at the Main Site

In this event, it is assumed that an incident has occurred but that degraded operations can be set up. In addition to the general steps that are followed in either case, special steps need to be taken.

- Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.
- Replace hardware as needed to restore service to at least a degraded service.
- Perform system installation as needed to restore service. If backup files are needed and are not available from the on-site backup files, they will be transferred from the off-site encrypted backup device.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the administration and users informed of the status, progress and problems.

Network Communications

Redundancy is being built into the computer communications systems.

This plan does not, at this time, address the problem of a need for redundancy in the telephone system. Considerable funds will be needed for an alternate plan in this area in case of a major disaster in the school telephone switching equipment. Most of the telephone and computer communications lines are in conduits across School, connecting lines to the schools IT infrastructure to boost performance and reliability across the phone system platform. In the event of a disaster a VoIP system can be diverted to a mobile phone to limit downtime. All incoming calls can be diverted in a short time to keep communication going.

Telephony - Disaster Recovery

In the event of a serious incident resulting in the loss of telephone communication the alternate means of direct communication for key personnel will be via personal mobile phones or email as listed:

1.---

2.---

3.---

4.---

5.---

6.---

7.---

8.---

9.---

10.--

Communication for key data will be via the IT Systems Manager’s laptop, until systems are back to a degraded or normal condition.

Appendix A

Background

The ICT computer network consists of a number of servers with a mixture of Windows Server 2008R2\2012R2 and Linux Servers running on VMware Hypervisor ESXi 5.1/5.5, the school site has Internet connectivity, and wireless coverage.

Backup and Restore Procedures

The following documentation gives details of procedures for the recovery of data in circumstances where a catastrophic loss of data has occurred due to file server failure. There are a variety of reasons for file server failure including hardware/software conflicts and failure, accidental or deliberate damage, hacking and inexplicable failures normally called ‘Act of God failures'.

Backup operations are carried out at the main school site onto a network attached storage (NAS) device connected to a backup server hosting backup applications.The backups are scheduled to run each night, Monday to Friday, a further “full” backup of some servers is taken at the weekend. This device is setup on a raid 5 for data protection and redundancy. The device is located in lower school. Each weekend an encrypted device containing a backup of key systems is taken off-site by the IT Systems Manager. Each half term an encrypted device containing a full backup of key systems and user documents is taken off-site by the IT Systems Manager.

All backup and restore operations are undertaken by the IT Systems Manager.

The IT Support Team hold copies of keys for the server room.

Disclaimer

While every effort is made to ensure the integrity and security of data held on the network, the Network Team cannot accept responsibility for permanent loss of data arising from any cause. Users should, at all times, follow standard network usage procedures: particularly maintaining regular local copies of important files.

Signed: ______________________________________

Chair of Governors

Date: ______________________________________

Date of Review:______________________________________