APPENDIX 7

ICT Disaster Recovery Plan

This policy was approved and ratified by the

Finance and Resources Committee of

Cox Green School

on

10th October 2017

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
1.4	Finance & Resources Committee	10/10/17	10/10/17	Sept 2020

Index of Document

Purpose and Scope

Introduction

Cox Green School (CGS) has a highly computerised operational environment like most schools and businesses. This includes the use of computers/laptops, servers, printers/copiers and other devices such as phones and CCTV. A school-wide network connects these various systems together and provides communications to other services including access to the internet for external services. These systems provide a critical component to the day to day operation of the school.

The reliability of the IT and Network Systems (ITNS) has increased dramatically in the past years. System failures that do occur can normally be diagnosed and repaired or exchanged promptly. The design of the school server infrastructure is around redundant policies which provide the best reliability and uptime while remaining good value for money.

For the most part, the major problems that can cause ITNS to become inoperable for a length of time result from environmental problems or sophisticated cyber challenges. Various situations or incidents that can disable, partially or completely, or impair support of CGS's ITNS have been identified. A plan to deal with these situations is provided.

Almost any disaster will require special funding from CGS in order to allow the affected ITNS to be repaired or replaced. This policy assumes that these funds will be made available as needed, however proper approval will be obtained before any funds are committed for recovery.

Objectives/Constraints

A major objective of this document is to define general procedures for a contingency plan to allow recovery from disruption of ITNS. This disruption may come from total destruction of the school-site to something such as minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting CGS's ITNS. 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 support given to CGS clients from academic and administrative systems within the remit of the IT and Network Systems Team. Each department at CGS should develop their own internal plans to deal with manual operations should any ITNS services be disrupted. Departments should work with the IT and Network Systems Manager to identify procedures they can develop to support with these plans.

Arising threats from cyber criminals makes it increasingly hard to safeguard the ITNS services and as seen in the news it is near to impossible to protect against all threats, such as so called "zero-day" exploits. Further to this, it is not possible to provide a full and detailed list of every possible situation that could result in the interruption of ITNS services. The ITNS Manager reviews every situation individually and provide the best advice to the Senior Leadership Team (SLT) where possible to ensure a quick, cost effective and methodical restoration of ITNS services.

Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. The schools senior leadership team (SLT) will make any special decisions (IT technical decisions will be made by the ITNS Manager, unless they believe the decision impacts the running of the school beyond their responsibility) 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 and Network Systems Manager for a determination of the need to declare an incident. The Head Teacher will also be notified.

The school IT and Network 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 Business Manager 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 affecting any CGS ITNS service 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 ITNS services 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 ITNS facilities for a period of 24 hours.

2. An incident which has impaired the use of computers or ITNS 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 data.

Contingencies

General situations that can destroy or interrupt the IT 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, Business Manager and Site Manager have access to the keys. The room is air conditioned and monitored by the school intruder and 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 a deadlock 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 ITNS 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

Incidents that cause major networking problems would require failure or damage to the server room, its equipment, fibre optic cables between this and each core network cabinet or core networking equipment.

All fibre optic cabling is installed in containment and where the route is external this is armored cable in external containment. The school has fibre optic specialist contractors available to replace any damaged cabling.

A disaster recovery server cabinet has been setup in another building the other side of the school site. In the event of an incident rendering the main server room inoperable, the primary servers can be brought online at this location.

Core networking equipment is covered by a lifetime warranty.

CGS has several suppliers who can provide essential server room equipment next day, to ensure essential services are restored as quickly as possible. Non essential equipment can be sourced with a longer lead time to ensure the best value for money.

Major telephone or Internet problems

CGSs telephone system is hosted in the server room, the system is covered with a 24/7 support contract to the service provider. The telephone service is covered by a 4 hour response time. The phone system itself and the main reception phone along with the emergency phones are covered by battery backup which will run the system for up to 4 hours in the event of lost power.

CGSs internet connection is on a 4 hour response 24/7 support contract. The school hosts the firewall equipment and have full management over the configuration. The firewall is on a support contract with the vendor. In the event of loss of internet, the IT and Network Systems team can easily identify the problem and contact the relevant support team to start restoration.

Environmental problems (air conditioning, electrical, fire)

An external maintenance company periodically services the air conditioning units, any faults are reported to and repaired by the maintenance company. The server room air conditioning unit is specified above capacity for the room to ensure the unit is not over worked. The external compressor is located in a secure location to avoid malicious damage. The air conditioning service company are available to respond out of hours if necessary. The school has a company that can provide temporary air conditioning units to the server room next morning if required while replacement parts/units are sourced.

Electrical

The server room has its own distribution board directly from the mains electrical cupboard, the shunt is clearly marked to ensure it is not isolated by accident. Having a dedicated supply for the server room allows other electrical works to take place around the school without compromising the supply to the room.

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. Automatic notifications are sent to the IT and Network Systems Manager in this event.

Fire

All server rooms are equipped with appropriate 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 fire alarm 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 stored outside of our main server room. Each weekend a full backup of all servers and data is taken off site on an encrypted device by the IT Network

and Systems Manager. This sufficiently protects the school systems and data from a full site disaster, allowing restoring of data to new or alternative equipment.

Insurance Considerations

All major hardware is covered under CGS's 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 determine a location to 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 Network and Systems Manager will serve as ICT Disaster Recovery Coordinator. In the event the IT Network and Systems Manager is incapacitated or unavailable, the school Business Manager will serve as ICT Disaster Recovery Coordinator and the most senior ITNS team member will take responsibility of Assistant ICT Disaster Recovery Coordinator to provide technical responsibility. 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 and Network Systems Manager and ITNS team will keep staff and students informed of the recovery activities. Where possible this communication will come from the Business Manager to enable the ITNS team to remain on task.

The IT and Network Systems Manager will be responsible for:

- Coordinating hardware and software replacement with the hardware and software vendors.

- Coordinating the activities of moving backup media and materials from the off-site backup and using these for recovery as and 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 backups contains adequate and timely server backup's and documentation for applications 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 devices.
- 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 data are backed up weekly.

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 school 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 and Network 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 IT Network 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, key personnel carry hand held radios which work on and around the school site. If these fail or should communication be

required to personnel off-site the alternate means of direct communication for key personnel will be via personal mobile phones as listed:

1.-Mr Tom Smith – IT and Network Systems Manager----------

2.-Mr Scott Andrews – IT and Network Systems Technician----------

3.-Ms Frances Walsh – Headteacher----------

4.-Mrs Gill Newman – Business Manager----------

5.-Mrs Caroline Dunne – Deputy Business Manager (Finance)----------

6.-Ms Cathrin Thomas – Deputy Headteacher----------

7.-Mr Ed Hillyard – Deputy Headteacher----------

8.-Mr Eric Teeder – Site Manager----------

9.-Mr Alan Cox – Site Controller (On-Site)----------

10.-Mrs Jane Doarks – HR and Administration Manager----------

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

Appendix A

Background

The IT server infrastructure our all hosted on virtual hosts. This enables quick and easier backup and restoration to new hardware.

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 server failure. There are a variety of reasons for 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. The backups are scheduled to run each night, Monday to Friday, a further "full" backup of servers is taken at the weekend. This device is setup on a raid 5 for data protection and redundancy.. Each weekend an encrypted devices containing a backup is taken off-site by the IT and Network Systems Manager. Each half term an encrypted device containing a full backup is stored offline

and stored for an entire academic year. At the end of each academic year a full backup is taken offline and stored on an encrypted device and stored for up to 7 years.

All backup and restore operations are undertaken by the IT and Network Systems Manager or an authorised member of the ITNS team.

Disclaimer

While every effort is made to ensure the integrity and security of data held on the network, the school 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 except where the data is business of the school, then this should not be taken off the school systems without the explicit permission of the IT and Network Systems Manager and the Business Manager.