Birkenhead Sixth Form College
IT Disaster Recovery Plan

Author:	John Paul Szkudlapski
Role:	Head of IT Services
Version:	3.2
Date:	11/05/2016
Status:	Pending Approval

Introduction

Since the mid-1990s Birkenhead Sixth Form College (the 'College') has increasingly come to depend on a large and sophisticated curriculum computer network. The curriculum network is a central and vital component of the college supporting some 1900 computing devices (desktops, laptops, tablets, MFDs, Telephones) and 1500 users. The college-wide network ties various file sharing, printing, email and internet systems together and provides support for the college Finance and CIS systems.

IT Services are located on the 1st Floor of the Hub, with the Head of IT Services being on the 2nd Floor of the Hub. The servers that control the network are located in 2 different rooms across the college (to mitigate total failure). These are all secure and air conditioned rooms. A backup server is located within the Art building comms cabinet (essentially a 3rd Server room) – this is because it is the furthese point from the main core network infrastructure. Despite increasing size and complexity, the reliability of our network has been consistently high for many years.

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 the College IT facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require special funding from the College in order to allow the affected systems to be repaired or replaced. The plan assumes that these funds will be made available, from insurance company or college funds, as required. 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 a server room or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents however special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the College including providing support to curriculum activities relying on computer systems. Consideration is given to recovery within a reasonable time and within cost constraints.

All production servers that are vital for the daily operation of the College are maintained under hardware service contracts with the equipment vendors. This ensures that routine maintenance problems will be addressed in a timely way.

Assumptions

This section contains some general assumptions, but cannot include all possible particular situations that can occur. Particular decisions for situations not covered in this plan needed at the time of an incident will be made by appropriate staff members on site.

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 Head of IT Services for a determination of the need to declare an incident. The Principal & Deputy Principal will also be notified.

The most senior IT Services staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have occurred as a result of the incident, immediate attention will be given to those persons injured. The Estates team will be notified. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., but evacuation and individual safety are the highest priorities.

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 College authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue to be the top priority until workable computer support to the College has been re-established.

Incidents Requiring Action

The IT disaster recovery plan will be invoked when there is an actual or threatened circumstances that will result in ‘significant impairment’ of the curricumlum and/or administrative systems that the IT Services team manages. This could include:

1. An incident which has disabled or will disable, partially or completely, the curriculum network facilities for a period exceeding one business day.

2. The loss of data that significantly exceeds the normal day to day restoration of student/staff files.

3. An incident that has significantly impaired the use of computers and networks managed by IT Services due to circumstances which fall beyond the normal processing of day-to-day operations.

4. The treat of significant loss of data, systems or facilities.

5. An incident which was caused by problems with computers and/or networks managed by IT Services and has resulted in the injury of one or more persons.

Possible Contingencies: Areas of Risk

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

- Power/Air Conditioning Interruption
- Fire
- Water ingress
- Weather and Natural Phenomenon
- Malicious damage (sabotage, hacking)
- Denial of service or virus attack

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 at an alternate site.
- Full recovery - operating at the current main college site possibly with a degraded level of service for a period of time.

Physical Safeguards

All server rooms are protected by Card Access Door Entry (Currently Paxton Net2) with a secondary Yale Lock. All IT Services and Caretaking staff have a key for these rooms.

Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist recovery from most types and levels of disruptive incidents that may involve 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.

Temperature Control (air conditioning)
Air conditioning units are the responsibility of Estates. The IT Services team periodically check the functioning of the air conditioning in server rooms. Any faults are reported to the Estates team who would call in a suitable contractor, if necessary. Air Conditioning units in all server rooms (including Art Block Backup Cabinet) are subject to a 4 month service/maintenance check by the college approved contractor.

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 by a sufficient amount to ensure the servers could be gracefully shut down in the event of a second power failure.

Fire

All rooms are equipped with manual CO_2 fire extinguishers, which will adequately protect the equipment from fires starting in the room itself. If a fire starts, the equipment could be used to limit damage to the affected piece of equipment and possible minor damage to equipment in the immediate vicinity. This would be handled as described in the preceding section:

In the event of a catastrophic fire involving the entire building, we would most likely have to replace all our hardware. Our critical servers are backed up constantly throughout the day (dependant on the server/data is varies between 15 minute intervals and 2 hour intervals). The college has a rocirpical offisite backup agreement with Carmel College, that sees our Offisite backup stored in their secure server room.

Insurance Considerations

All major hardware is covered under the College's standard Property and Casualty insurance for the College.

Security Strategies

The college employs standard security strategies. For example by, as far as possible, using standard software, hardware & local and wide area networking components. This includes Microsoft software on all Computing Devices, Windows Server software, switches and also routers. This industry standard approach will in itself permit reasonable mitigation of outage through market reliability and knowledge.

JISC firewall technology is employed (a) to prevent "rogue" access to the college network and resources and (b) to ensure the college network is employed for educational purposes, however the college recognises that our networks are increasingly "open" systems and like all networks are vulnerable to unauthorised access and that our information can be damaged by malicious individuals or carelessness. The College also uses two Sophos UTM perimeter firewalls which are also deployed by a number of major police forces throughout the UK.

Network security is a major consideration in our systems design. All our servers and workstations have automated systems to maintain them with up to date antivirus definitions and operating system updates.

We recognise that we cannot achieve "absolute" security across all aspects of our activities. Questions relating to the cost/benefit balance in security matters will be addressed and formally reviewed centrally to allow curriculum and administrative users to perform their activities freely in the understanding that, for the most part, the security risks have been assessed and addressed corporately.

Individual users shall be made aware of their responsibilities with regard to how they can contribute to the overall security level. Guidance on good practice shall be provided to all users (curriculum and administrative, staff and students) and correspondingly special efforts shall be directed to those who are handling particularly sensitive information such as student record information, personnel information and financial information.

A system is in place to ensure the prompt removal of access rights, and the removal of data, of staff and students on leaving.

The College shall ensure that business continuity plans are in place to ensure that all systems and networks have appropriate plans and recovery strategies for major breakdown, loss of network facilities or data. This includes plans to recover data, test our restore systems, source replacement servers, network and other critical components.

IT Disaster Recovery Team

Possession of IT Disaster Recovery Plan

The primary copy of the IT Disaster Recovery Plan is held in the IT Services folder on the public drive on the College Network. Soft and hard copies of the Plan will be kept by the Principal, Deputy Principal, The SMT member responsible for Estates and the Estates Manager. Copies are also held by all members of IT Services.

IT Disaster Recovery Team Base

In the event of a disaster the recovery team will meet as follows:

1. If The Hub is usable, the recovery team will meet in the office of the Head of IT Services.

2. If The Hub is not usable, the recovery team will meet in an appropriately safe location.

3. If the college facilities are not usable then it is presumed that the disaster is of such proportions that recovery of IT facilities will take a lesser priority. The head of IT Services will make suitable arrangements.

IT Disaster Recovery Manager

The Head of IT Services will act as the IT Disaster Recovery Manager. In their absence the IT Support Officers will assume joint authority.

Responsibilities of the IT Disaster Recovery Manager

The major responsibilities are:

- Determining the extent and seriousness of the disaster, notifying SMT and the CIS Manager immediately and keeping them informed of the activities and recovery progress.
- Invoking the IT Disaster Recovery Plan after approval from SMT.
- Supervising the recovery activities.
- Coordinating with the CIS Manager and other members of the College Senior Management Team on priorities while going from partial to full recovery.
- The Disaster Recovery Manager will keep staff informed of the recovery activities. Staff in turn will update students where appropriate.
- Coordinating hardware and software replacement with the hardware and software vendors.
- Coordinating the activities of moving backup media and materials from the off-site security files and using these for recovery when needed.
- Keeping SMT and the CIS Manager of the extent of damage and recovery procedures being implemented.
- Coordinating recovery with departments, those using the academic computers and/or those using business functions.
- Coordinating appropriate computer and communications recovery.

Preparations for a disaster

This section contains the 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 storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

General Procedures

Responsibilities have been given for ensuring each of following actions have been taken and that any updating needed is continued.

The Head of IT Services is responsible for

- maintaining, reviewing and updating the IT disaster recovery plan.
- Ensuring that all members of IT Services receive copies of the Plan and are given the opportunity to discuss its implications.

- Ensuring that procedures are in place to ensure both our onsite and offsite backup systems are periodically checked and tested.
- Maintaining and periodically updating IT disaster recovery materials, specifically documentation and systems information (electronically and manually).
- Maintaining a current asset register of equipment.
- Ensuring that UPS systems are functioning properly and that they are being checked periodically.
- Ensuring that the College is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.
- Ensuring that the proper environment is maintained in server areas.

Recovery Procedures

This portion of the disaster/recovery plan will be set into motion when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode in a reasonable time.

It is assumed a disaster has occurred and the Critical Incident Plan is to be put in effect. This decision will be made by the Principal \ Deputy Principal upon advice from the IT Disaster Recovery Co-coordinator.

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.
- Notify vendor systems support personnel that help is needed immediately to begin procedures to restore systems software.
- Order any additional electrical cables needed from suppliers.

- Rush order any essential technical supplies 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 alternate site:

- Coordinate moving of equipment and IT support personnel into the alternate site.
- Bring the recovery materials from the off-site storage to the alternate site.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Prepare backup materials and return these to the off-site storage area.
- Set up operations in the alternate site.
- Coordinate activities to ensure the most critical jobs are being supported as needed.
- As alternate site provision is utilised, ensure that periodic backup procedures are being followed and materials are being placed in off-site storage periodically.
- Work out plans to ensure all critical support will be phased in.
- Keep SMT and staff informed of the status, progress, and problems.
- Coordinate the longer range plans with SMT of continuing support and ultimately restoring the overall system
- To ensure that if a breach of security has occurred that any access points are secured and passwords changed.

Degraded operations

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 storage.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the SMT informed of the status, progress and problems.

Appendix 1 – Data Back Ups and Restoration

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'.

The following documentation gives details of our backup procedures and will enable the recovery of data in circumstances where a catastrophic loss of data has occurred due to file server failure. All our backups are run with a verify option and test restorations are performed

We are able to restore any user file to the form it was the previous evening or to go back in time to 'any week this month or any month in the last three' to restore corrupted user files or system components.

Schedule

Two types of backups are taken during the college day.

Type A – Snapshot
Dependant on the server/data a backup is taken automatically every 15 mins or upto every 2 hours and takes a 'snapshot' of the network. All college servers are interrogated to identify those files which have changed since the last snapshot. These files are then backed up to hard disks.

Type B – End of Day
Scheduled to occur at night time, this backup is a full copy of everything on the college network. Files are written to our offsite backup system at Carmel College which backs up any changes since the previous day. This facility enables us to retain data for a lot longer offsite.

Appendix 2 – Testing Proceudres

It would be impractical to simulate an actual disaster on the entire college network as this would require the creation of a temporary server room with enough servers to recover the main college systems. This would be expensive and very time consuming.a more suitable approach would be to simulate a disaster in one particular area of the college network. The network can be sectioned into eight separate areas.

They are:

- Internet Access
- Staff E-Mail
- Student Data
- Staff Data
- Core Network Servers

- Print Services
- Wireless
- CIS

Therefore approximately every six weeks one of these areas would be restored fully from backup onto a disaster recovery server. This would simulate a disaster in part of the college network without the requirement of taking the area offline. The college network is so fully utilised that taking it offline to simulate a disaster would cause too much disruption.

However, after a disaster has occurred it would be necessary to resort from backup anyway and therefore this test will adequately provide a suitable testing platform for our services.

Appendix 3 – Internet Links

The JANET internet link is maintained by JISC and all problems should be reported directly to them.

Janet Service Desk	0300 300 2212 / operations@ja.net

Appendix 4 – Staff Emergency Contact Details

0151 652 5575 – College Reception

Name	Role	Mobile
John Paul Szkudlapski (Head of IT Services)	IT Disaster Recovery Manager	07734 694525
Dave Maple (IT Support Officer)	Disaster Recovery Team	TBA
Liam Bridge (IT Support Officer)	Disaster Recovery Team	TBA
Mike Kilbride (Deputy Principal)	Disaster Recovery Team (SMT Contact)	TBA