

IT Disaster Recovery Action Plan



Reviewed by: Ian Bingle

Governing Body

8th November 2008

Whaley Bridge Primary School

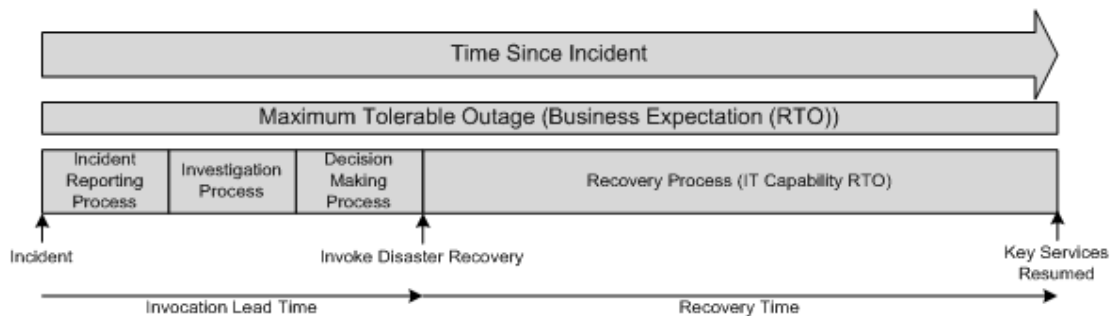
1.0 INTRODUCTION

Whaley Bridge Primary School (WBPS) utilises Information Technology (IT) in many aspects of the school management and in educational preparation, delivery and review. Over time, IT services have become critical to overall school performance. As a result of this ever-increasing reliance on technology, WBPS require a comprehensive IT Disaster Recovery Plan to assure these services can be quickly and completely re-established in event of an incident.

An incident in the above context can range from complete loss of the school facility (where this plan would feed into and bolster the school's critical incident plan) to the loss of an individual component (PC, network, software environment, etc.) to the loss of important data (X files, financial data source, anything not easily reproduced).

In preparing this plan it is important to note that the expectation is that in the normal course of events, systems will fail, data will be lost, mistakes will be made, service delivery will be intermittent, etc. As such, not every incident will be categorised as a "disaster". This is the norm and any plan should seek to establish mechanisms that will see things restored back to the status quo within defined and acceptable time frames which will vary depending upon the individual components. Only when restoration will exceed the maximum tolerable outage (MTO) would a **disaster** normally be declared.

The actual time to restore a component from an incident is only one part of the overall MTO. The plan needs to take into account detection time and other management processes prior to invoking the recovery process.



Restoration of individual components will involve some amount of effort and technical knowhow that may and probably will lie external to the existing school staff. Where this is the case, these resources need to understand and commit to this plan if its objectives are going to be met.

This plan summarises the results of a comprehensive risk analysis conducted for all IT components; it provides general steps that will be taken in event of a disaster to restore IT functions; and it provides recommendations for "hardening" of the IT infrastructure that may require management approval and additional funding to implement.

Whaley Bridge Primary School

2.0 OBJECTIVES

The primary objective of this IT Disaster Recovery Plan is to help ensure continuity of service for WBPS by providing the ability to successfully recover computer services/data in the event of a disaster.

Specific goals of this plan relative to an emergency include:

- Detailing a general course of action to follow in the event of a disaster,
- Minimising confusion, errors, and expense to the school, and
- Implementing a quick and complete recovery of services.

Secondary objectives of this Plan are:

- Reducing risks of loss of services/data,
- Providing ongoing protection of components, and
- Ensuring the continued viability of this plan.

3.0 ROLES

The following Roles have been identified and report to the Headmaster of WBPS (or Senior Management Nominee):

- **IT Disaster Plan Co-ordinator (ITDPC):** An individual appointed by the Headmaster that owns and manages this plan on behalf of the school.
- **Infrastructure Manager:** An individual or 3rd party company that undertakes defined IT functions on behalf of the school.

The following Roles have been identified and report (on a technical basis) to the Infrastructure Manager:

- **Hardware Vendor:** 3rd party companies that supply IT hardware on a commercial basis for the school use.
- **Software Supplier:** 3rd party companies that provide software on commercial basis for school use.
- **LEA IT Support:** County based services on which WBPS depend (network, security, firewall, email, SPAM, content filtering, remote backup, etc).

4.0 SCOPE

This plan will only address the recovery of systems under the direct control of WBPS and assumes (rightly or wrongly) that the services “bought in” from the LEA and other providers have their own IT Disaster Recovery and Business Continuity Plans in place for the services that they provide. In reality, this is a pragmatic assumption short of the school committing to the expense of dual sourcing these components. It is suggested that when testing this overall plan, these 3rd party services are specifically and regularly “exercised”.

Also, given the uncertain impact of a given incident or disaster, it is not the intent of this document to provide specific recovery instructions for every system. Rather, this document will outline a general recovery process which will lead to development of specific responses to any given incident or disaster.

Whaley Bridge Primary School

This plan recognises that its implementation cannot happen over-night and that the school, Governing Body, LEA and 3rd party suppliers will need to work over time to make this plan a reality. In the interim, local DR initiatives, backup regimes for critical files/data, etc. already in operation should continue “as is” until the **ITDPC** specifically indicates those activities are redundant.

5.0 ASSUMPTIONS

This disaster recovery plan is based on the following assumptions:

- Once an incident covered by this plan has been declared a **disaster**, the appropriate priority will be given to the recovery effort and the resources and support required as outlined in this IT Disaster Recovery Plan will be made available.
- Depending on the severity of the disaster, all users of IT may be required to modify their operations to accommodate changes in system performance, computer availability and physical location until a full recovery has been completed.
- 3rd party bought in services (such as network access to LEA systems, the internet broadband, service etc.) come with adequate protection against malicious software, viruses, trojans and security compromise at source (school firewall?) rather than the school having to specifically protect each individual computing resource.
- Where school computing resources may access other networks (e.g.) laptops or data, programmes or files are able to be loaded onto school computing resources (via external VPN access, memory sticks, CD's, floppies, etc.), then these devices are similarly and individually protected against malicious software, viruses, trojans and security compromise.
- No 3rd party computing devices (personal laptops, mobile computing devices, etc) are allowed to gain access to the school network (physical or wireless) or gain any form of peer to peer network connection, unless specifically audited and authorised by the **ITDPC**.

6.0 DEFINITIONS

The following definitions pertain to their use in this IT Disaster Recovery Plan:

- **Backup/Recovery Data:** Copies of all software and data deemed critical or valuable. This data will originate on the central server(s). The backup and recovery data will exist in separate file systems and may be held locally and remotely to the school. The backup data is used to return the servers to a state of readiness and operation that existed shortly prior to the incident/disaster.
- **Disaster:** A significant or unusual incident that has long-term implications to the working of the WBPS whereby the maximum tolerable outage (MTO) has or will (in the opinion of the **ITDPC**) been exceeded.
- **Incident:** An event which impacts a specific IT service, server or data.
- **Level 1 Risk:** Risk associated with the loss of the **most** critical IT services, capabilities, applications or data.
- **Level 2 Risk:** Risk associated with the loss of or impairment to critical IT services, capabilities, applications or data.
- **Level 3 Risk:** Risk associated with the loss of other identified IT services, capabilities, applications or data.

IT Disaster Recovery Action Plan

Whaley Bridge Primary School

7.0 RESPONSIBILITIES

The **ITDPC** is responsible for:

- **Management of this plan**
And in particular management of the Infrastructure Manager
- **IT Contacts Register**
The school will maintain a contact list for all suppliers (hardware, software, service, advisors, insurer's) that have an impact on this plan. This should also seek encompass similar institutions that have agreed to provide reciprocal shared services to the school in an emergency.
- **Establishing SLA's**
Suppliers of hardware, software and particularly service elements of this plan need to be able to commit to responding in timeframes that allow the school to meet the defined MTO's, Where possible this should be written into their existing service level agreements or contracts with the school.

The **Infrastructure Manager** is responsible for (but not necessarily personally undertaking):

- **System Audit**
Definition and documentation of all key components on the system (including information for insurers), upgrade status, the licence information, network shares, whether standard or custom built, basic hardware level, file system types.
- **System Build/Restoration**
Restoring from image or re-install disks, upgrading to latest software levels, restoring users, restoring networking & network access, restoring file access & privileges.
- **System Maintenance**
Keeping software revisions up to date as per software providers' recommendations, upgrading the OS with latest patches/service packs, registry cleaning, file system integrity checking/defragmenting.
- **System Security**
Maintaining virus protection, email scanning, personal firewall (for mobile devices), phishing, spyware & intrusion protection, user access rights & privileges, system password rotation, user password strength & regime, VPN access control, wi-fi lockdown.
- **Data Access Control**
Setting up user based roles and access to appropriate data and maintaining those rights on any utilised backup devices.
- **Backup/Restore**
Ensuring the central server(s) have hardware RAID protection against individual disk failure. Local backups to be conducted to external network attached storage device. Remote backups to be conducted to County servers (when service becomes available and affordable) or to 2nd network attached storage device which can be accessed by VPN or locally and then removed off site (with adequate controls on data security if a 3rd party).
Setting up and monitoring success of full and incremental backup regimes for all critical & valuable data secured on the central server(s).
Copies of master software disks should be made (usually allowable as part of the licence agreement) and stored off school premises.
- **Local DR Testing**
Undertake a quarterly local DR test in isolation of the school critical incident plan that encompasses a system build and restoration of "lost data". Actual and successful occurrences of such a task performed in the normal course of events (when adequately

Whaley Bridge Primary School

documented) to count towards this exercise.

- **Plan Update**

The output of the DR testing (live or simulated) should be used as a trigger to validate and adjust this plan on an ad hoc basis as should the introduction of significantly new or different IT systems to the school. Outside of these triggers, this plan should be reviewed annually.

8.0 GENERAL DISASTER RESPONSE & RECOVERY GUIDELINES

Data that is deemed critical or valuable will be held on the school's intranet to facilitate regular centralised backup and management of systems.

Data access to the centralised server(s) is done by standardised named "shares" and access rights to sensitive data controlled by user based privileges.

No critical or valuable data will be held on local computing devices unless local backup arrangement is in place & functional (memory sticks, local external disks, etc.) and authorised by the **ITDPC**. This backup data is to be held separately & securely from the original source.

Wherever possible (and where licensing permits) computers of similar function should be of a standard & documented build allowing fast rebuild from a system image. Rebuild or upgrade of these systems should be regular to maintain the operating system and key software components to the provider's specification.

Non standard build IT equipment will be audited to ensure that:

- Key software utilities are identified to facilitate system restoration.
- Software revision levels of the operating system and other key software components are maintained to the provider's specifications.
- Copies of the software licence are available for use in future restoration activities.

In the event of a non obvious disaster, the **ITDPC** will notify the Headmaster.

The **ITDPC** will identify individuals required to assist in the recovery process.

The school will be informed as to IT system degradation and restrictions on IT usage and/or availability.

The **ITDPC** will develop an overall IT recovery plan and schedule, focusing on the school's highest priorities as defined by the component **Risk Level**.

Necessary software and hardware replacement will be coordinated with vendors and the school's insurer.

The **ITDPC** will communicate recovery status updates to the Headmaster.

The **ITDPC** will verify restoration of the IT infrastructure to pre-disaster functionality.

Whaley Bridge Primary School

9.0 IT RISK ASSESSMENT

For each main area of IT usage (Computer Suite, ER Building, Administration PCs/Servers, Headmaster's PC, Classroom PC, School Laptops, Library, Offsite backup systems), IT Risk assessments will be performed by the ITDRC covering:

- **General**
Description of the IT in place (PCs, printers, scanners, networking, storage) its function(s), users, capability, use for private/sensitive/controlled data
- **Physical/Security Risks**
Access doors, windows, public/private space, lockable room, alarms, security cables, video surveillance.
- **Environmental Risk**
Flooding (flat roof, ground floor plumbing, fire system), fire, extreme temperatures (inc a/c)
- **Internal Systems Risk**
Networking infrastructure, cabling
- **External Systems Risk**
Power, BT communications, Internet Service provision, quality of software updates

- **Recovery Planning**
Alternate space, systems, service provision, shared services available
- **Risk Assessment Level**
Level 1, 2 or 3
- **MTO Definition**
The time at which the loss of this service, facility or data would be declared outside the scope of normal expected and planned for acceptable failure and be considered a "disaster" that warranted immediate attention.
- **Estimated time to procure replacement**
Hardware (and or software if media destroyed).
- **Estimated time to recover to new hardware**
Rebuild of systems from scratch or from system images and re-establishment of data, links to data and other services
- **Requirement for Resiliency/Back-up**
None
Hardware RAID storage system
Backup – local, offsite, both
Backup regime – Full/Incremental
Data Sensitivity – User Access Control or Encryption.
- **Preventative & further measures required**
Identify **measured and proportionate** improvements to current facilities which will serve to reduce risks. Suggest a timescale for agreement and implementation so that items can be prioritised correctly

While it may be that having conducted risk assessments, it is determined that the loss of much of the IT infrastructure individually (classroom PC) or in larger groups (library) would have only minor impact to the teaching of management of the school, it will at least serve to highlight those **key** components which should be the subject of the higher priority activities for prevention and for DR testing.