MLT Disaster Recovery Plan

Date Last Reviewed: September 2016
Reviewed by: ICT Team Leader
Approved by: CEO
Next Review Due: September 2018

Maltby Learning Trust

IT DISASTER RECOVERY TEAM

In the event of an IT related disaster:

1.1 The IT DRP Co-ordinator is contacted and in his absence another member of the IT DRP team will take his place.

1.2 The DRP Co-ordinator contacts the IT support team and relevant technical members of IT DRP team.

1.3 An assessment (written or verbal) of the extent of the damage will be made by the group.

1.4 The group reports back to the IT DRP team.

1.5 Decisions are made by the team as to the short term and long term actions required to resume IT services. The team will use the service priority list (detailed below) and advice from team members to decide on the order of operations. The order of priority may fluctuate to respond to key programmes of activity indicated on the Academy calendar. The Principal in consultation with the governing body will have the responsibility for determining priorities of work.

1.6 If required, emergency funds will be made available by the Trust to purchase essential equipment.

Role	Person	Contact details
IT DRP Co-ordinator	E Price	07774 326051
IT DRP Team	S Hatherley	07468 466856
IT DRP Team	T Nuttall	07547 605434
SLT representatives	G Hayward	07595 608406
Partner schools representatives	D Orridge (Ecclesfield School)	01142 409591
	I MacMillan (Wales Academy)	01909 771291

In the event of the IT support team being unavailable. Partner schools have been asked to supply technical support team members.

The team should consider the following when deciding on the order of operations:

1. Continuity of the staff and student experience.
2. Security/Safety of students and staff.
3. Proximity to coursework deadline dates.
4. Exam entry data integrity.
5. Online exam dates.
6. Integrity of financial information.

Note:-

Since server hardware identical to present systems are unlikely to be available at restore time, physical servers will be built as new or server systems moved to a virtual environment. This will allow for quicker initial recovery but full system functionality may take considerably longer.

The present services and their priority are listed below

Service	Brief explanation	Priority
Networking	Ability to connect to and shared resources/files with other ICT. Ensure secure and efficient access to network via wired and wireless technology	1
Data storage	Access to a database. A database is used for MIS (SIMS) and many curriculum based applications	2
Document storage	Ability to save files either locally on the machine or removable media and on a file server (depends on networking)	3
E-mail	Ability to access e-mail (requires internet access)	4
Software Applications	Application software, also known as an application, is computer software designed to help the user to perform singular or multiple related specific tasks. Examples include enterprise software, accounting software, office suites, graphics software, and media players. Curriculum Software MIS and Finance Software	4
		2
Client machine	Maintain, re-image computers.	5
Internet	Offer secure, monitored access to the internet and on-line resources.	6
Web	Ability to host web services (intranet etc)	7
Security	Anti-virus – Counter measures for virus attacks Backups - Copy of data if information is lost or damaged	8
Printing	Ability to print documents	9

In the event of total destruction of all services and buildings the team should consider:-

1. A location for the DR team to meet and co-ordinate work. E.g. Partner school, LA, feeder school depending on the nature of the disaster

2. Contacting partner schools, through the head teacher or SLT, to restore or relocate IT essential lessons and services to IT suites and offices within these facilities.
3. Contacting feeder schools, through the head teacher or SLT, to restore or relocate essential IT lessons to IT suites within these facilities.

LIKELY SCENARIOS

1. Power loss to B&E block
2. Power spike in B&E block
3. Fire in server room
4. Flood in server room

In all cases the following should be undertaken:-

Once the problem has been identified basic information is needed to allow for a decision to be made as to the next step. This information should comprise:

a) The servers affected
b) The server functions
c) Is the infrastructure intact? If not what is the extent of the damage.
d) Can the machine be reused (is it just disc damage or is the machine unusable)
e) Are funds available to replace damaged systems?
f) Are spares available from partner schools for short term solutions?
g) Are most recent backups available?

The **risk register** details possible service discontinuity scenarios, risk levels, risk treatment, mitigation techniques, an estimate of service recovery targets and the approximate cost to restore the service. This will be used to aid decision making during the recovery process.

2. FURTHER INFORMATION/GUIDANCE

- Loss of the switches in certain areas (because of the infrastructure topology) will result in loss of all networking functionality.
- Lead time for acquisition of servers is usually 10 working days but IBM have agreed, through our lead supplier, that in a disaster scenario, delivery time would be less than 5 days.
- An assessment will need to be made as to the effect of each server on the functioning of the school. Priority will then be given to the rebuild of each machine.
- Virtualisation technology can be used in some areas to restore services quickly but systems restored may not be up to date.

- A decision will need to be made, if we cannot wait 5/10 days for the new servers, to take a less critical server off line and rebuild them as an interim step.
- Partner schools have offered support both in terms of IT equipment and man power.
- A pool of server software is available which can be used to rebuild machines if required. This is held in the cloud on Microsoft's servers.

3.   BACKUP PROCEDURE INFORMATION

See Maltby Learning Trust Backup policy.