ICT Disaster Recovery Policy

Updated:	July 2023
Next Review Date:	July 2025

The following are situations that would affect the functionality of Cambridge School network system and their proposed solution.

Please note that backups are taken of all critical servers and data – below is a link to the backup information for Cambridge School:

Cloud Based Communication with Parents, Pupils and Staff

The school uses a cloud based company (Parentmail) to communicate with parents and staff. There is an automatic update link between the schools MIS system and the website to ensure the most up to date information is accessible from any machine with internet access.

Whole School Power Failure

Effect - Critical

Should the school suffer a complete power failure then all the computers would shut down. The servers have uninterruptible power supplies (UPS) and would shut themselves down automatically after 15 minutes. The UPS's would safely shutdown the servers resulting in no loss of server data. All files opened at the time that is not already saved to the servers would be lost – we expect this to be minimal.

A whole school power failure for any length of time would result in the closure of the school until the situation was resolved. Once the power was restored the server should startup automatically.

Solution: School need to liaise with the utilities power supplier to determine the seriousness of the problem and the downtime.

Downtime – Unknown

Partial Power Failure – Studio Block – Non Serious

A failure of the power supply to the Studio Block would result loss of use of ICT equipment within this space.

Solution: Office space will be shared within the main building to accommodate the therapy team. The curriculum will be changed slightly, moving classes into the main building until the problem was rectified**.**

Partial Power Failure – Server Room – Critical

A failure of power to the Server Room would result in the failure of the whole network due to the loss of the core switches.

Solution: Failing checking onsite fuseboxes, School need to liaise with an electrician to determine the seriousness of the problem and the downtime.

Failure of Network Switches

This would result in network downtime and systems being unavailable until functionality has been restored. Users affected would depending on what switch has the issue – each switch serves a different part of the building. The core switch which is connected to all other switches would affect all network services in the school.

Solution: Following the I.T Support providers assess and emergency onsite visit, if a temporary switch cannot be provided, a replacement Switch would be ordered for next day delivery.

Downtime – 1 day depending on scenario.

Failure of Host server

The failure of the host server would result in all virtual servers it hosts being offline which would affect all I.T services – nothing would be available. The server is currently configured to alert the I.T Support provider on system warnings / issues prior to failure. Several components are configured with redundancy (2 power supplies on the server, hard drive redundancy etc) and so the failure of the entire system without notice is unlikely.

Solution: The server is covered with a next business day warranty for all components. In the event of a failure, following the I.T Support providers assessment and emergency onsite visit, the support provider will contact the server manufacturer (Dell) to trigger the warranty service. Depending on the time of day, this will be scheduled for the next business day or the day after.

Downtime – 1-2 days.

Failure of Backup Server
Effect – High
The failure of the Backup server would not allow us to backup or recover data.
Solution: I.T support provider would remotely repair or reconfigure a new server to take over Backup services. The Backup is hosted on a separate device to the server as well as in the cloud so loss of data is extremely unlikely.

Downtime – 1 day

Failure of Router
Effect – Severe

Loss of internet and email access. Internal network services would be available.

Solution: The main router is the property of LGFL and as such we have no control over repair times. The I.T Support provider would be contacted and they will liaise with LGFL in order for them to resolve.

Downtime – Unknown.

Fire in Main Building
Effect – Critical
A fire in Main Building would be the most serious situation for the computer network as this is the location of the Server Room containing all the servers and core switches, and most of the major ICT suites.

Solution: School would be required to trigger insurance policies in order to replace equipment based on asset register information etc. Network switches can be replaced in a day but the LGFL internet equipment and cabling would be subject to LGFL response times. A new server usually arrives within 1-2 weeks. Data is backed up to a NAS device in the studio building to mitigate fire risk, however, in the event this was affected by the fire, the backed up data is also replicated in the cloud. The I.T Support provider would be required to restore the network from the backup once the server was onsite. We would be able to get limited access to other buildings within 2-3 days but full access would be 7-14 days. Restoring the server room and Network rooms would be dependent on the level of destruction.

The main delay would be restoring the infrastructure of the building.

Downtime – 7 – 14 days once fire damage has been repaired.

Fire in Other Blocks – Serious
Chance of failure - <0.1% Effect - High
A fire in another building would require restoration of the infrastructure.

Solution: Restore the building infrastructure as soon as possible. ICT equipment could be bought within 7 days. Cabling would take longer.
Downtime – 7 – 14 days once fire damage has been repaired.