**APPENDIX B**

ICT Disaster Recovery and Business Continuity Plan

Langley Fitzurse Primary School

Updated 4 December 2019

Table of Contents

[1. Overview 3](#_Toc412118950)

[1.1 Purpose and scope of this plan 3](#_Toc412118951)

[1.2 How the plan is activated 3](#_Toc412118952)

[1.3 Keeping the plan up to date 3](#_Toc412118953)

[1.4 Security of document 3](#_Toc412118954)

[1.5 Distribution List 4](#_Toc412118955)

[2. Disaster Recovery Plan 5](#_Toc412118956)

[2.1 Network Infrastructure 5](#_Toc412118957)

[2.2 Wireless Infrastructure 5](#_Toc412118958)

[2.3 Servers 5](#_Toc412118959)

[2.4 Virus Infection 5](#_Toc412118960)

[2.5 Backup Strategy 5](#_Toc412118961)

[2.6 Power 6](#_Toc412118962)

[2.7 SIMS 6](#_Toc412118963)

[2.8 Passwords 6](#_Toc412118964)

[3. Critical Systems 6](#_Toc412118965)

[3.1 Category 1 Systems 6](#_Toc412118966)

[3.2 Category 2 Systems 7](#_Toc412118967)

[3.3 Category 3 Systems 7](#_Toc412118968)

[4. Disaster Recover Command Centre 7](#_Toc412118969)

[5. Testing the plan 8](#_Toc412118970)

[6. Vendor and Supplier Contacts 9](#_Toc412118971)

[7. Risk Assessment and Business Impact Review 10](#_Toc412118972)

Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date Issued | Issued by | Update Details |
| 0.1 | 16.11.2015 | OJG | 1st draft |
| 0.2 | 30.11.2016 | OJG | Following Review on 25.11.16 |
| 1.0 | 04.12.2019 | OJG | Major update |
|  |  |  |  |
|  |  |  |  |

# Overview

The purpose of this plan is to bring together all of the required information that will be needed in the event of a serious disruption of ICT services at Langley Fitzurse Primary School. This plan covers only disruption to the ICT services and should be read in conjunction with other school disaster recovery plans.

## Purpose and scope of this plan

“For the purposes of this plan a Disaster is defined as loss or damage of part or all of the schools ICT Infrastructure, which would have a high, or very high, business impact on the school.”

Disaster, as outlined in the above definition, includes:

1. Total loss of site, (e.g. due to fire damage)
2. Loss or technical failure of one or more network servers
3. Loss or technical failure of network infrastructure i.e. hub/switch/router/comms link
4. Extended loss of electrical power
5. Failure of a key software system

Key software systems which are specifically referred to in this plan include:

1. SIMS – Management Information System
2. Exchange Email system

The purpose of this plan is to reinstate the ICT facilities with the minimum time possible and to minimise disruption to the school population.

## How the plan is activated

In the event that a disaster is identified by the Senior Leadership Team (SLT) they or their appointed deputy will be responsible for activating the plan and monitoring the progress of disaster recovery procedures, reporting to SLT and undertaking any further action as necessary.

## Keeping the plan up to date

It is essential that this plan is kept up to date and should be reviewed at least every twelve months or immediately after any significant changes to the ICT system are made.

It is the responsibility of the SLT to ensure that the details and procedures within this document are adhered to and up to date.

## Security of document

This document contains highly confidential information and must be kept securely by the copy holders. Each copy of the document will be numbered sequentially and the SLT will keep a record of who has what copy.

## Distribution List

The SLT is responsible for distributing this plan according to the table below. Each recipient will receive two copies; one copy is to be kept securely at the place of work and the other copy at their home or other secure offsite location.

A copy of this plan will also be kept on the Oakford Portal which is hosted in a geographically separate location from the school and is available, securely, to authorised Oakford employees.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Position** | **Contact Number** | **Copy Number** |
| Oakford Technology Ltd | IT Support | 01380 888088 | 1 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Disaster Recovery Plan

## Network Infrastructure

The network infrastructure is based on a combination of Gigabit core switches and edge POE switches. There is no redundancy in the network design and every switch represents a single point of failure.

The network switch configuration is currently flat and so no backup of the switch configuration is required.

As part of the IT support agreement, Oakford Technology are able to loan network switches in the event of a failure.

## Wireless Infrastructure

The wireless network is based on HP Aruba access points configured to provide wireless LAN services to school owned and managed laptops and devices. Access points used are the HP Aruba IAP range.

The configuration of the HP Aruba access points is backed up and maintained centrally by the Oakford on site support engineer
.

## Servers

The central server infrastructure is fully virtualised using Hyper-V technology.

The Hyper-V 2016 host server was supplied by Oakford Technology and is covered by a hardware maintenance warranty. The server contains the school’s SIMS data, Staff files, Student files, Admin files, RDS server (remote access) and deployment services. The host server does not use Hyper-V replication at present. In the event of server failure and loss of its associated virtual machines, the server hardware would need to be replaced or repaired, virtual machines and system re-setup, then data restored.

## Virus Infection

In the event of a catastrophic viral infection the server will need to be rebuild using installation media. Once this has been completed the data restoration will be started. (ESET licence key distributed from Oakford Technology)

## Backup Strategy

Backups take place every week night. All relevant data from virtual servers is backed up nightly using an Oakford Technology provided remote backup solution.

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **Backup Offsite (frequency)** | **Notes** | **Retention Policy** |
| OakfordSRV | Daily | Staff, Admin and Student Data |  28 days by default. Change to 90 days in July to cover the summer holiday |
| OakfordSIMS | Daily | SIMS and FMS Data |  28 days. Change to 90 days in July to cover the summer holiday |
| OakfordDS | N/A | Computer deployment files | N/A |
| OakfordTS | N/A | Remote access server | N/A |

## Power

All of the servers and broadband equipment are protected from power interruptions by a UPS (uninterruptable power supply). The UPS ensures that there is a period of time that the ICT systems can continue to operate without mains power. Nominally this period of time is at least 5 minutes.

## SIMS

SIMS support is provided via Oakford/School ICT 3rd party helpdesk.

##  Passwords

Domain passwords are held by the Oakford Network Support Team in Devizes in an encrypted vault.

# Critical Systems

The schools systems are divided into three different categories as defined below. Systems in each category are defined within the sections below.

|  |  |
| --- | --- |
| **Category** | **Definition** |
| Category 1 | Essential to running of school |
| Category 2 | Important to running of school |
| Category 3 | Important to teaching within school |

## Category 1 Systems

|  |  |  |  |
| --- | --- | --- | --- |
| **System / Application** | **Users affected** | **Recovery timescale hardware** | **Recovery timescale software** |
| Oakford Server Host | All | 1 - 2 days | 7 -14 days |
| Core Switch | All | < 2 days | NA |
| Edge Switches | Certain rooms | < 2 days | NA |
| Desktops / Laptops | Individual users | < 5 days | < 2 days |
| SIMS / FMS | Staff | < 3 days | 7 - 14 days |
| Exchange Online (email) | All | N/A | < 1 day |
| File and print servers | All | < 3 day | < 3 days |
| Active Directory | All | < 3 day | < 2 days |
| Broadband | All | < 3 day  | N/A |

## Category 2 Systems

|  |  |  |  |
| --- | --- | --- | --- |
| **System / Application** | **Users affected** | **Recovery timescale hardware** | **Recovery timescale software** |
| Microsoft Office | All | NA | < 2 days  |
| Wireless Network | Curriculum | < 2 days | < 2 days |
|  |  |  |  |
|  |  |  |  |

## Category 3 Systems

|  |  |  |  |
| --- | --- | --- | --- |
| **System / Application** | **Users affected** | **Recovery timescale hardware** | **Recovery timescale software** |
| User applications | Staff/Students | <7 days | <2 days |
|  |  |  |  |

# Disaster Recover Command Centre

In the event of a catastrophic disaster, the recovery operation will be managed from the command centre, as defined in the Langley Fitzurse Primary School disaster recovery plan.

In the event that availability of this facility is also affected by the disaster the command centre will move offsite to the Oakford Devizes office at 10, Prince Maurice Court, Devizes, Wiltshire. SN10 2RT.

# Testing the plan

It is essential that each of the various elements of this plan are tested to ensure that in the event of an actual disaster, systems can be recovered in line with this plan with a minimal interruption to users.

It will not be necessary to fully test the plan for all of the virtual servers because the recovery procedure is the same for each. However, it is considered important that each system which has a different procedure for recovery is tested. Therefore following tests should be carried out:

• Fully test of all the UPS equipment to ensure correct operation, notification and sufficient battery life.

Wherever possible these tests should be carried out during normal office hours, and not involve any downtime of live servers during core working hours. In addition to these tests, the following should be carried out regularly:

• Test restores from disk to ensure that backups are reliable

• Tests of UPS systems to ensure they are functioning correctly

It is imperative that backups are checked daily to ensure they are operating correctly. Automated emails will be generated daily detailing success or failure of individual backup jobs.

The IT team are to test random data restores at least twice per year.

# Vendor and Supplier Contacts

|  |  |  |  |
| --- | --- | --- | --- |
| **Area of responsibility** | **Contact** | **Contact (working hours)** | **Contact (outside working hours)** |
| PCs, Laptops, Tablets, Networking | Oakford | 01380 888088 | 07796173810 |
| Oakford Servers, Desktops | Oakford | 01380 888088 | 07796173810 |
| Internet | Oakford | 01380 888088 | 07796173810 |
| SIMS | SchoolICT | 0345 2226802 | N/A |
| Backups | Oakford | 01380 888088 | 07796173810 |

# Risk Assessment and Business Impact Review

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood / Severity | Negligible(1) | Minor(2) | Moderate(3) | Major (4) | Extreme(5) |
| Rare (1) | Low | Low | Low | Low | Medium |
| Unlikely (2) | Low | Low | Medium | Medium | High |
| Possible (3) | Low | Medium | Medium | High | High |
| Likely (4) | Low | Medium | High | High | Very high |
| Almost Certain (5) | Medium | High | High | Very high | Very high |

| **Location** | **Network Element** | **Type of loss / damage** | **Likelihood** | **Severity** | **Business Impact** | **Precautions in place** |
| --- | --- | --- | --- | --- | --- | --- |
| LANGLEY FITZURSE PRIMARY SCHOOL | Host servers | FireTheftWater DamageVandalismWindAccidental | 1 | 5 | Loss of the entire Hyper V system would cause significant impact on the school. | Servers are in a secured room.Backups of all systems are taken daily.  |
|  |  | Component failure: hard disk  | 3 | 1 | No impact from loss of a single hard disk.The impact of the loss of all disks would be as per fire, theft above. | All servers are protected via RAID5 data drives.RAID tools will report disk failure |
|  |  | Component failure: network card | 3 | 1 | No impact from loss of single network card | Network connections are duplicated (x2)  |
|  |  | Component failure: fan | 3 | 1 | No impact from loss of single fan | Fans are duplicated |
|  |  | Component failure: power supply | 3 | 1 | No impact from loss of single power supply | Power supplies are duplicated |
|  | HP ProCurve Core switch | FireTheftWater DamageVandalismWindAccidental | 1 | 5 | Loss of any switch would cause significant impact on the school | HP Switches are in secure cabinet |
|  |  | Component failure: fan | 3 | 1 | No impact from loss of single fan | HP support |
|  |  | Component failure: power supply | 3 | 5 | Main network switch has single power supply. Failure would take down the entire network. | HP support |
|  | HP Edge Switch | FireTheftWater DamageVandalismWindAccidental | 1 | 3 | Loss of a single switch will leave all devices connected to that switch without network access. | HP Support. |
|  |  | Component failure | 3 | 3 | Loss of a single switch will leave all devices connected to that switch without network access. | HP Support. |
|  | UPS | FireTheftWater DamageVandalismWindAccidental | 1 | 2 | Loss of UPS leaves devices connected to that switch vulnerable to power outages. | UPS are in secured room. APC supportUPS duplicated |
|  |  | Component failure: battery | 3 | 2 | Loss of UPS leaves devices connected to that switch vulnerable to power outages. | UPS are in secured room. APC supportUPS duplicated |
|  | Broadband Router | FireTheftWater DamageVandalismWindAccidental | 1 | 5 | Loss of Router would cause significant impact on the school and a complete loss of Internet connection | This equipment is provided by OakfordConfiguration is backed up off site. |