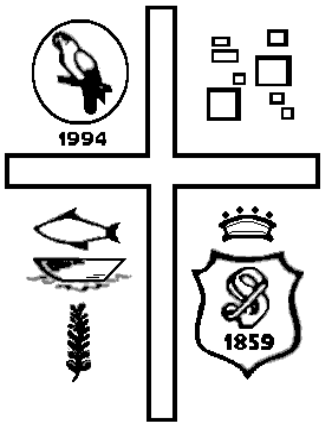
The Curzon Church of England Primary School



The Curzon Primary School – ICT Disaster Recovery Plan

March 24
Review March 27

The Curzon Primary School – ICT Disaster Recovery Plan

Updated 10.3.24

Introduction

The purpose of this document is to set in place strategies to ensure the secure backup and recovery of important data that is stored on the school administration and curriculum networks. The data to backup includes school management data files, administration network user documents, teaching staff documents and pupil documents. The strategies in place will be robust enough to ensure the recovery of data in any circumstances.

Identified risks are:

- Fire or flood
- Electrical failure or surge
- Catastrophic hardware (including portable media) or software failure
- Virus or hacker attack
- Accidental damage to hardware
- Theft of hardware
- Accidental file deletion

Data can be destroyed by system malfunction or accidental or intentional means. The ongoing availability of important data is critical to the operation of the school. To minimise any potential loss or corruption of this data, individuals responsible for providing and operating administrative applications need to ensure that data is adequately backed up by establishing and following an appropriate system backup procedure.

Disaster Recovery

Admin PCs are covered by a full hardware and software maintenance contract with Derbyshire County Council IT Services Division.

The school network and IT equipment is managed and maintained by a Derbyshire County Council Engineer that has passed all CRB/Disclosure Barring requirements, who attends the school 6 days over the year to maintain the equipment (this is usually DCC). The engineer can be contacted via their mobile or the school can phone 01629 537777 option 1 in the event of a breakdown.

All computers, laptops, iPads, and other IT equipment etc. are listed on the School Inventory with serial numbers and other relevant information. These inventories are maintained regularly by the school business manager. Software licences are listed and kept within the school.

In the event of an internet outage the school are to contact KCOM (internet provider) or Ekte (web filtering), or Capita (DNS)

School Data

All data created within the school is stored on the School's Office 365 tenancy in SharePoints and users' individual OneDrive's.

Files are recoverable from the Deleted items in the relevant areas, and version history can be used to revert to earlier versions on the file.

Management Information System (RM Integris)

The admin staff and the Headteacher have access to RM Integris which is password protected with unique usernames. All teachers have access to RM Integris for pupil registration and other add-ons as and when they become available. Access to the system is limited to known individuals via passwords. The above authorised personnel have access to children's and parents' data.

Finance System

SAP is web based and in accordance with the Financial Regulations and Procedures, only the admin staff and the headteacher have access rights according to their level of approval.

Network

The school now operates a serverless environment, with all data and operations now held in the Microsoft cloud. The school's devices are managed by Microsoft Intune.

All teachers and teaching assistants have access to the Office 365 tenancy and are allocated unique usernames that are password protected to ensure there is individual accountability for all activity on the network.

GDPR

Any devices that leave the school are encrypted with BitLocker (with a PIN). Recovery keys are held centrally within the school's Office 365 tenancy.