turn IT on
Connecting schools and technology

tel: 01865 597620
web: www.turniton.co.uk
email: office@turniton.co.uk
post: Wittas House, Two Rivers, Station Lane, Witney, OX28 4BH

Turn IT on IT Disaster Recovery Plan

The Charter Schools Educational Trust

1.0 INTRODUCTION

The Charter Schools Educational Trust (the 'Trust') utilises Information Technology (IT) in many aspects of school management and educational preparation, delivery and review.

IT services are critical to overall school performance. As a result of this ever-increasing reliance on technology, turn IT on (TIO) have a comprehensive IT Disaster Recovery Plan. For the Trust this plan will be implemented when required for the following schools:

- Charter North
- Charter Bermondsey
- Lyndhurst Primary
- The Belham Primary
- Dulwich Hamlet Junior School
- Streatham Wells Primary
- Charles Dickens Primary
- Loughborough Primary School
- The Charter School East Dulwich (from September 2026)

An incident in the above context can range from complete loss of the school facility to the loss of an individual component (PC, network, software environment, etc.) to the loss of important data (current files, archived files, financial data sources, etc).

Not every incident will be categorised as a 'disaster'. This is normal practice, 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.

2.0 OBJECTIVES

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

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.

3.0 KEY NETWORK COMPONENTS

Listed below is an overview of the key operational servers that the school have on each site, each is considered to be critical in the smooth running of the network. The list includes both physical and virtual servers.

3.1 SERVER OVERVIEW

School	Server Name	IP Address	Description
Charter North Dulwich	**Physical:**		
	TCS-HOST-01	10.16.165.101	Failover Host 1
	TCS-HOST-02	10.16.165.102	Failover Host 2
	TCS-VEEAM	10.16.165.125	Veeam Backup Server
	Virtual Servers:		
	TCS-SR-001	10.16.165.10	DHCP, DNS, AD
	TCS-SR-002	10.16.165.4	
	TCSHost-DC01	10.16.165.103	TCSHost Domain
	TCSHost-DC02	10.16.165.104	Controller
	CCR	10.16.165.20	TCSHost Failover DC
	PAXTON	10.16.176.148	Catering Company Server Paxton Net2- Access Control
Charter Bermondsey	**Physical:**		
	VH-SRV-01	10.20.170.131	Host 1
	VH-SRV-01	10.20.170.132	Host 2
	Virtual Servers:		
	COMP-DC-01	10.20.170.133	DC, DHCP, DNS, MDT
	COMP-FILE-01	10.20.170.141	File Server – Home Drives
	COMP-LIB-01	10.20.170.138	Library software
	COMP-BIO-01	10.20.170.137	Catering Company
	COMP-PRT-01	10.20.170.134	Print Server – PaperCut MF
	compsims01	10.20.170.135	School MIS
Lyndhurst Primary	**Physical:**		

	LPS-HOST **Virtual Servers:** LPS-DC LPS-FILES	10.16.60.20 10.16.60.10 10.16.60.11	Host Server DC, DHCP, DNS File server
The Belham Primary	**Physical:** BPS-SVR-HYPERV1 **Virtual Servers:** BPS-SVR-DC1 BPS-SVR-DC2 BPS-SVR-FILE1 BPS-SVR-NET2	 10.18.72.25 10.18.72.31 10.18.72.32 10.18.72.33 10.18.72.51	 Host Server DC, DHCP, DNS DC, DHCP, DNS File Server Paxton Net2- Access Control
Dulwich Hamlet Junior School	**Physical:** DHS-Core **Virtual Servers:** DHS-SVR-01 DHS-PRT	 10.17.191.250 10.17.191.252 10.17.191.245	 Host Server DC, DHCP, DNS Print Server - PaperCut
Streatham Wells Primary	**Physical:** SV-HYPERV **Virtual Servers:** SV-DC01 SV-APP01 SV-DATA01	 10.171.188.120 10.171.188.2 10.171.188.6 10.171.188.5	 Host Server DC, DHCP, DNS Paxton Net2- Access Control File Server
Charles Dickens Primary	**Physical:** CDS-HOST **Virtual Servers:** CDS-DC CDS-FILES CDS-ACCESSCONTROL	 10.17.100.178 10.17.96.3 10.17.96.4 10.17.96.6	 Host Server DC, DHCP, DNS File Server Paxton Net2- Access Control
Loughborough Primary School	**Physical:** LPSRVR01 sims-server2023 **Virtual Servers:**	 10.170.164.2 10.170.164.3	 Host Server School MIS
The Charter School East Dulwich - to be	**Physical:** **Virtual Servers:**		

completed from September 2026			

3.2. VIRTUAL SERVERS

School	Server Name	IP Address	Description

4.0 UNDERSTANDING AND DEFINING DISRUPTION OF SERVICE

Objective	Actions/Considerations
Confirm the nature of the disruption	What has happened? When did it occur? Which systems and/or services are affected? How potentially serious is it? What is the estimated duration of the problem? Who else has been informed (staff/ suppliers / customers)?
Decide whether to invoke Network Infrastructure Recovery plan	The decision will be based upon the information provided consideration should be given to: How long systems will be unavailable? Whether the systems affected are required to support the business priorities? Whether the area is currently responding to an external incident? Inform staff that the Business Continuity Plan is being invoked or put staff on standby or invoke agreed manual systems to ensure that the service can continue to operate. If the decision is made not to invoke the plan, continue to monitor the situation until such time as normal service is resumed.

5.0 KEY CONTACTS

5.1 SCHOOL STAFF

Name	Company	Job Title	Office Contact
Cassie Buchanan	Charter Trust	CEO	07540 880259
Shalene Varcoe	Charter Trust	Head of Governance and Compliance	07969 071209
Charlie Evans	Charter Trust	Director of Estates	07738 078744
Andrew Lynn	Charter Trust	CFO	07903 526268
Mahen Padayachee	Charter Trust	Trust Head of IT	07840 162997
Mark Pain	TCSND	Headteacher	07736 121064
Alison Harbottle	TCSED	Headteacher	07837 633535
Marcus Huntley	CSB	Principal	07950 923482
Ally Sprakes	BPS	Headteacher	07863 663977
Michael Eggleton	CDPS	Headteacher	07469 190929
Tom Turnham	LPS	Headteacher	07817 376963
Sarah Wordlaw	SWPS	Headteacher	07710 513061
Graziella Williams	LOU	Headteacher	07980 302903
Claire Purcell	DHJS	Headteacher	020 7525 9188
Sarah Botchway	LSTSH	Director	020 3935 4663

5.2 KEY SUPPORT AND THIRD-PARTY COMPANY CONTACTS

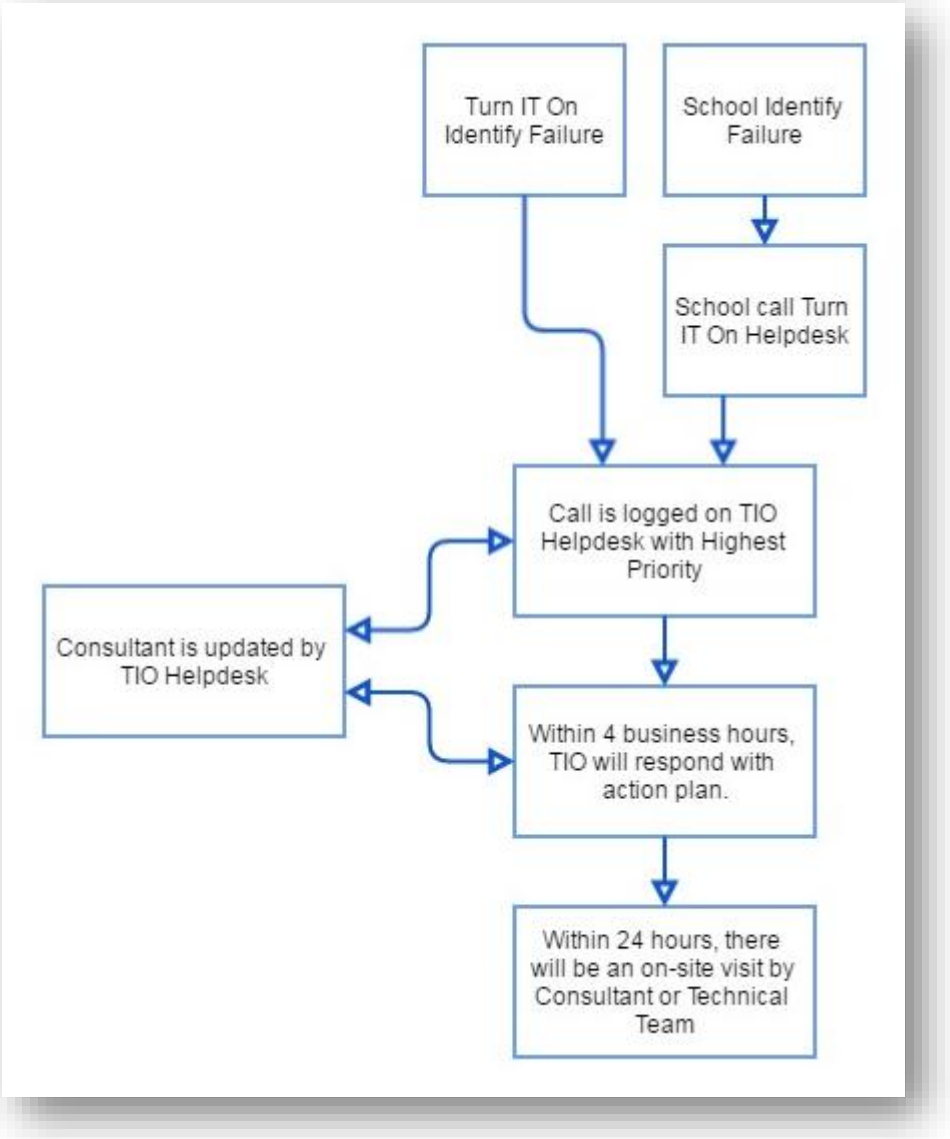
Company	Contact	Job Title/Service	Office Contact
Turn IT On	Main Office	IT Support	01865 597620
Turn IT On	Anna Fitzgerald	Regional Team Manager	07498 989707
Turn It On	Matt Reader	Commercial Manager	07950 860562
Turn it On	NEW – To be completed	IT Manager CND	
Turn it On	NEW – To be completed	IT Manager CED	
Turn it On	NEW – To be completed	IT Manager CSB	
Turn it ON	Savio Fernandes	IT Technician - Primaries	07706 332593
LGFL	Broadband provider plus filtering and monitoring services: https://helpdesk.lgfl.net/support/tickets/new?product=Escalation%20to%20LGfL		

6.0 PROCEDURES

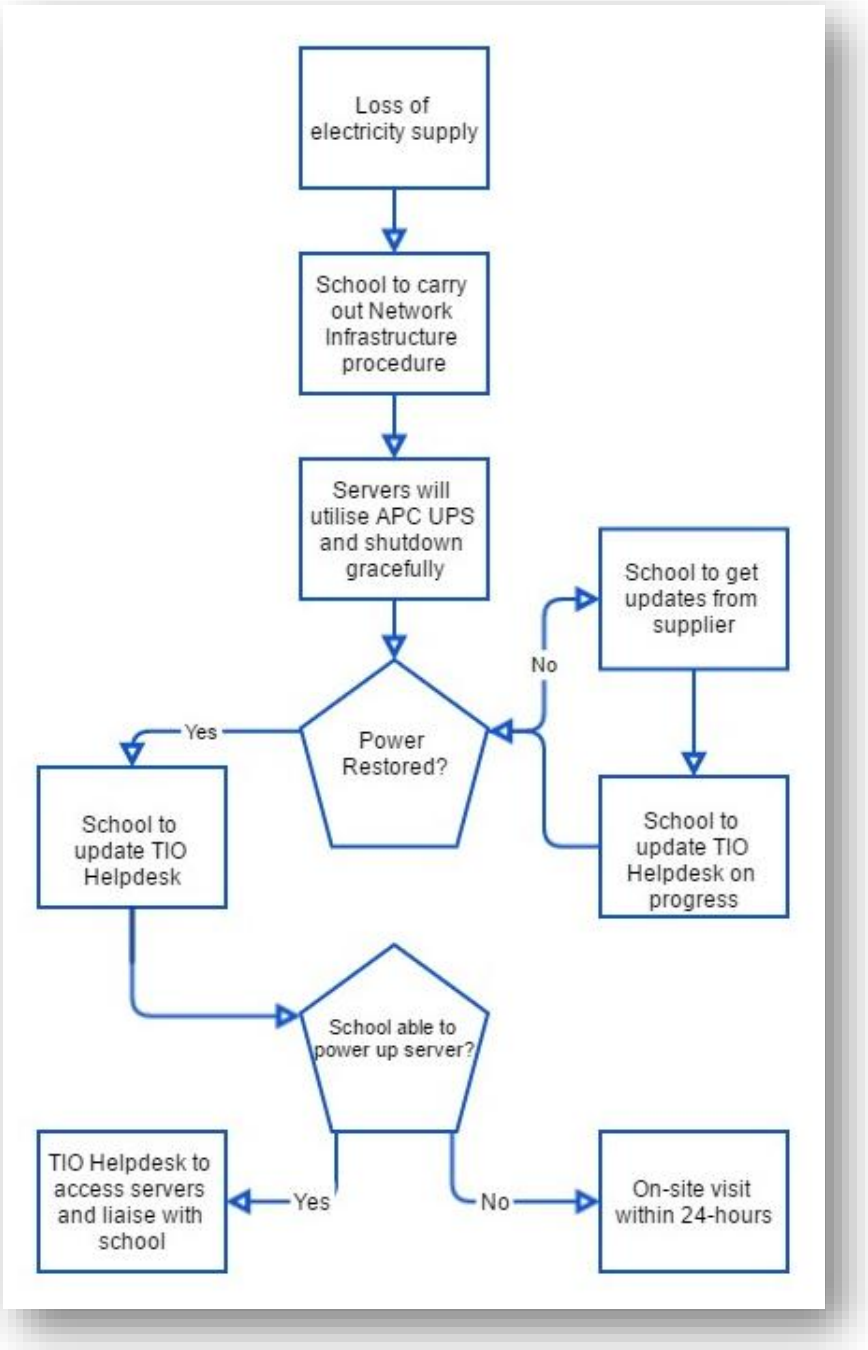
6.1 NETWORK INFRASTRUCTURE RECOVERY

The following procedure should be carried out to initiate Network Infrastructure Recovery:

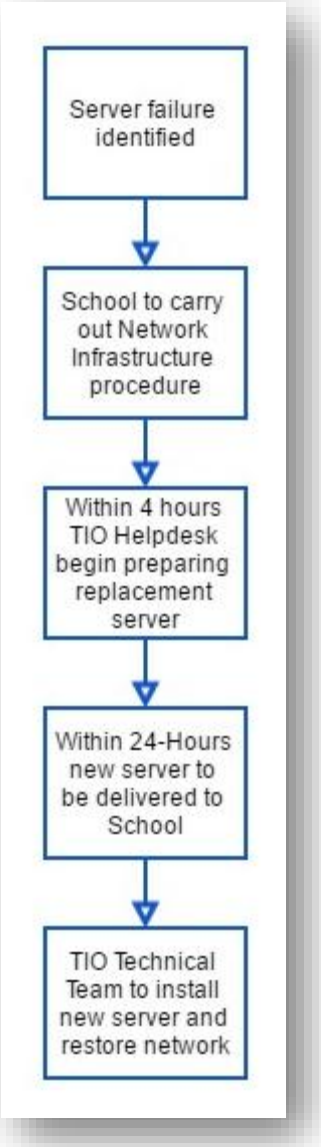
In the event of an identified network infrastructure failure, the school should call the Turn IT On Helpdesk as soon as possible.



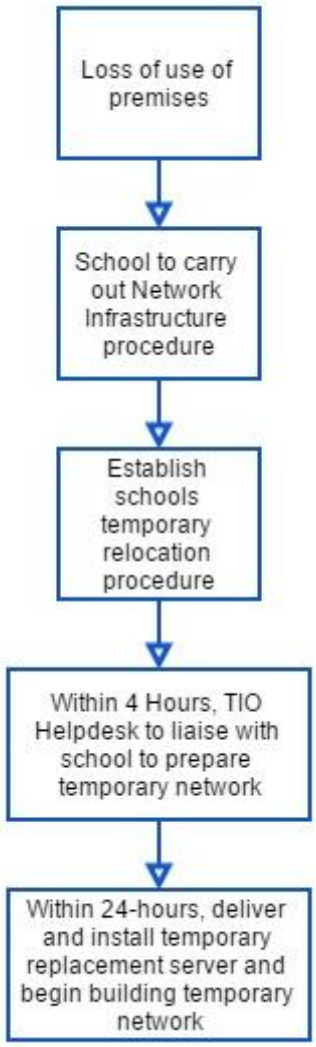
6.2 POWER LOSS



6.3 SERVER FAILURE



6.4 LOSS OF SCHOOL PREMISES



7.0 RANSOMWARE

Ransomware typically spreads via spam or phishing emails. It can also be spread through websites or drive-by downloads to infect an endpoint and penetrate the network. Infection methods are constantly evolving and there are many other ways users can become infected. Once in place, the Ransomware then locks all files it can access using strong encryption. Finally, the malware demands a ransom (typically payable in bitcoins) to decrypt the files and restore full operations to the affected IT systems.

Encrypting ransomware or Cryptoware is by far the most common recent variety of ransomware. Other types that might be encountered are:

- Non-encrypting ransomware or lock screens (restricts access to files and data, but does not encrypt them)
- Ransomware that encrypts the Master Boot Record (MBR) of a drive or Microsoft's NTFS, which prevents victims' computers from being booted up in a live OS environment
- Leakware or extortionware (exfiltrates data that the attackers threaten to release if ransom is not paid)
- Mobile Device Ransomware (infects cell-phones through drive-by downloads or fake apps)

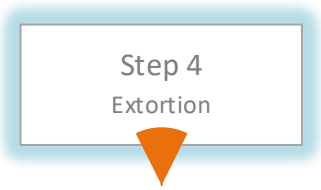
Steps in a Typical Ransomware attack:

Ransomware attacks come in many different forms but most currently follow a similar process after infection as below.

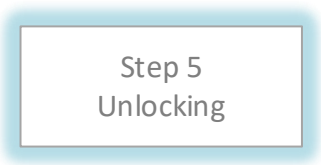
After it has been delivered to the system via email attachment, phishing email, infected application or other method, the ransomware installs itself on the endpoint and any network devices it can access.

The ransomware contacts the command and control server operated by the cybercriminals behind the attack to generate the cryptographic keys to be used on the local system.

The ransomware starts encrypting any files it can find on local machines and the network.



With the encryption work done, the ransomware displays instructions for extortion and ransom payment, threatening destruction of data if payment is not made.



Organizations can either pay the ransom (not recommended) and hope for the cybercriminals to actually decrypt the affected files (which in many cases does not happen), or they can attempt recovery by removing infected files and systems from the network and restoring data from clean backups.

Ransomware attacks target organisations of all sizes including schools — 5% or more of businesses in the top 10 industry sectors have been attacked — and no size business, from small-and-medium

businesses to enterprises, is immune. Attacks are on the rise in every sector and in every size of business. Schools are now high on the list and we are seeing increasing incidents.

The unfortunate truth is that ransomware has become so widespread that for most companies and schools it is a certainty that they will be exposed to some point to a ransomware or malware attack. The best they can do is to be prepared and understand the best ways to minimize the impact of ransomware. Therefore, we need to offer the best advise to protect against any form of attack.

Phishing emails, malicious email attachments, and visiting compromised websites have been common vehicles of infection, but other methods have become more common in past months. Weaknesses in Microsoft's Server Message Block (SMB) and Remote Desktop Protocol (RDP) have allowed cryptoworms to spread. Desktop applications — in one case an accounting package — and even Microsoft Office (Microsoft's Dynamic Data Exchange — DDE) have been the agents of infection.

Recent ransomware strains such as Petya, CryptoLocker, and WannaCry have incorporated worms to spread themselves across networks, earning the nickname, "cryptoworms."

Ransomware will never be eradicated and will adapt as companies and organisations fight to keep up with the threat, groups and individuals who use ransomware are generally one step ahead.

To be prepared, we need to know how ransomware can enter our systems. The methods of gaining access to systems are known as attack vectors.

Attack vectors can be divided into two types: human attack vectors and machine attack vectors which are outlined below:

Human attack vectors

Often, viruses need the help of humans to enter computers, so they employ what is known as social engineering. In the context of information security, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. In other words, people can be fooled into giving up information that they otherwise would not divulge.

Common human attack vectors include:

1. Phishing

Phishing uses fake emails to trick people into clicking on a link or opening an attachment that carries a malware payload. The email might be sent to one person or many within an organization. Sometimes the emails are targeted to make them seem more credible. The attackers take the time to research the individual targets and businesses, so their email appears legitimate. The sender might be faked to be someone known to the recipient or the subject matter relevant to the recipient's job. When personalized in this manner, the technique is known as spear phishing.

2. SMSishing

SMSishing uses text messages to get recipients to navigate to a site or enter personal information on their device. Common approaches use authentication messages or messages that appear to be from a

financial or other service provider. Some SMSishing ransomware attempt to propagate themselves by sending themselves to all contacts in the device's contacts list.

3. Vishing

In a similar manner to email and SMS, vishing uses voicemail to deceive the victim. The voicemail recipient is instructed to call a number that is often spoofed to appear legitimate. If the victim calls the number, he or she is taken through a series of actions to correct some made-up problem. The instructions include having the victim install malware on their computer. Cybercriminals can appear professional and employ sound effects and other means to appear legitimate. Like spear phishing, vishing can be targeted to an individual or company using information that the cybercriminals have collected.

4. Social Media

Social media can be a powerful vehicle to convince a victim to open a downloaded image from a social media site or take some other compromising action. The carrier might be music, video, or other active content that once opened infects the user's system.

5. Instant Messaging

Instant messaging clients can be hacked by cybercriminals and used to distribute malware to the victim's contact list. This technique was one of the methods used to distribute the Locky ransomware to unsuspecting recipients.

Machine Attack Vectors

The other type of attack vector is machine to machine. Humans are involved to some extent as they might facilitate the attack by visiting a website or using a computer, but the attack process is automated and does not require any explicit human cooperation to invade your computer or network.

1. Drive-By

Drive-by has this title because all it takes for the victim to become infected is to open a webpage with malicious code in an image or active content.

2. System Vulnerabilities

Cybercriminals learn the vulnerabilities of specific systems and exploit those vulnerabilities to break in and install ransomware on the machine. This most often happens to systems that are not patched with the latest security releases.

3. Malvertising

Malvertising is like drive-by but uses ads to deliver malware. These ads might be placed on search engines or popular social media sites in order to reach a large audience. A common host for malvertising is adults-only sites.

4. Network Propagation

However, a piece of ransomware enters a system, once it has it can scan for file shares and accessible computers and spread itself across the network or shared system. Companies without adequate security might have their company file server and other network shares infected as well. From there, the malware will spread as far as it can until it runs out of accessible systems or meets security barriers.

5. Propagation Through Shared Services

Online services such as file sharing or syncing services can be used to propagate ransomware. If the ransomware ends up in a shared folder on a home machine, the infection can be transferred to an office or to other connected machines. If the service is set to automatically sync when files are added or changed, as many file sharing services are, then a malicious virus can be widely propagated in just milliseconds.

It is important to be careful and consider the settings we use for systems that automatically sync, and to be cautious about sharing files with others unless we know exactly where they came from.

8.0 RECOVERY PROCEDURES

8.1 DATA RECOVERY

Back Up Systems Used & Recommended Procedures

Remote Backup - Online Backup

The school's data is backed up on a daily basis and Information is password protected, encrypted and stored off-site. In the case of server failure or theft then the school's data is protected. Files can be restored quickly via the backup software or if a large restore is needed, the backups can be shipped on-site.

Local Backup – TIO Discover NAS

Key servers are backed up including system files and data at the end of each workday to a local NAS device. This is best used for restoring individual files or in the case of a total server failure this backup can be used to restore the system from.

In the event of data loss, depending on the scenario these are the steps that would be followed:

In the event of partial server failure:

If the server has a failure which either causes a full or partial loss in access to data or services then the cause of the failure will be identified and replacements parts will be ordered and installed, depending on the type of failure there may not necessarily be a need for a restore from backups to take place.

In the event of total server failure or theft:

If the server suffers a total failure which is not recoverable (e.g. fire or other natural disaster), has been stolen or any other event which has caused a total failure of the server then a replacement unit will be ordered and installed. Once installed a complete restore from Windows Server Backups will be made to restore the service.

In the event of a Ransomware attack

The best method to recover form a ransomware attack is to restore the system from a clean backup.

Good backups and retention are the main defence against system vulnerabilities.

As a rule, we no not encourage payment for Ransomware. The risks associated with payment and non-return of data access are very high.

8.2 RANSOMWARE INCIDENT FOLLOW UP PROCEDURE

The following process should be followed a Ransomware incident has been identified.

1. Disconnect and stop all backup solutions to protect backup integrity. Cloud backups should be protected but its good practice to stop all backup services.
2. Disconnect and stop all user remote access solutions (not Datto)
3. Inform the central services team of the incident, a ticket will need to be raised but communication should be instant, a phone call to the central team is the best method and escalate if you do not get a response. A 3rd line Consultant will be allocated to assist with the incident.
4. Communication with the school is critical and should be a priority, inform key contacts at the school of the incident and follow up procedure. This communication should include information on how often we will update on progress. Clear communication with the school will help eliminate stress and frustration.
5. Work with the 3rd line team to investigate and plan to resolve the incident.
6. Investigate the incident and understand how Ransomware entered the network: It is critical we know how the Ransomware entered the system so we can patch vulnerabilities and make sure the system is safe before we continue with remedial work or a full system rebuild. Investigate which systems are affected by the incident, this should include servers, computers and mobile devices. Its good practice to disconnect all devices from the network before we commence remedial work, a single client device could reinfect the network if infected and not isolated.
7. In most cases we will need to rebuild the network and restore information from a reliable backup. Check the integrity of all backups to make sure we have recoverable data available.

Once we fully understand the implication of the incident and have all the information at hand, inform the school of the work involved and timescales to complete the work.

Work with the allocated 3rd line consultant to rebuild the network and bring the system back online. All risks highlighted during the initial investigation should be eliminated and removed from the system moving forward.

Full user testing should be undertaken after the system has been recovered as with all system builds and major work.

The school may require a summary statement on what has happened and what steps have been taken to mitigate any future risk.

All ransomware incidents should be logged as a potential data breach by the school under the GDPR.