# **Backup Strategy**

# In order to test restoration processes, it is essential that you first have a robust and clearly defined backup strategy. Your backup processes should fit with your school business needs and be tested routinely.

Backups protect your school against data corruption caused by system outage, software/application errors, database corruption and accidental deletion. Off-site backups are a vital defence against malware.

Please refer to additional guidance available on the [Education Data Hub](https://educationdatahub.org.uk/cyber-resilience/) website for sample disaster recovery and incident response plans.

**Remember:**

* Data is live, backup solutions are not, therefore data restored may not contain all the data at the point of outage.
* Even a disk mirror takes time with large volumes over high speed connections.

Business Continuity / Critical Incident Planning:

* Policy and vision
* Keep critical school functions operational
* Reducing overall impact of interruption
* Defining backup and restore methods

Advanced planning should prevent the need for disaster recovery.

IT Disaster Recovery Planning:

* Procedures and resources
* Responding to disasters and disruptions
* Developing emergency response procedures
* Reducing the impact of immediate dangers
* Restoring critical IT systems

Disaster Recovery required when business continuity planning has failed

# **Data Recovery**

Restoring data and systems from backup is the first stage.

Just because data is not on IT systems / servers does not mean it doesn’t exist. There could be paper files / notes / records on email systems and logs. The data can be manually or technically recovered by the business.

The time for this is called the **Recovery Window.**

# **Essential Objectives**

**Recovery Point objective (RPO)** - sets out how old the most recent backup can be before the level of data loss would be too great for the school to operate. The RPO affects the backup strategy directly.

This timeframe may be different for different systems. A tracking system may be updated several times a year, for example, whilst an MIS will be updated daily.

**Recovery Time Objective (RTO)** specifies how quickly systems must be recovered for you to be operational again. Unless the school tests backup restoration and recovery processes, SLT and governors will not know if they can meet the necessary timescales, or even if recovery works at all.

**Maximum Tolerable Outage (MTO)** is the maximum amount of time that a system or facility can be unavailable before significant disruption or damage occurs.

# **Stages of Restoration**

The business service before the incident needs to be replicated and the following three stages apply:

* **RESUME**
* **RESTORE**
* **RECOVER**

1. Business as Usual: Within the normal teaching and learning delivery
2. Incident: Service outage but still normal
3. Disaster Invoked: New disaster affecting teaching and learning delivery
4. IT Restoration IT systems working from backup for critical/High priority systems

(Restore Point Objective – **RPO**)

1. Business Recovery: Restoration to recovery for normal core education delivery

(Recovery Time Objective - **RTO**)

1. Resumption: Getting everything back to working order – ‘business as usual’

(Meeting the Maximum Tolerable Outage – **MTO**)