# JOHN TAYLOR MULTI ACADEMY TRUST

# ICT Security Backup Policy

Reviewed: October 2019

**Version Control**

| Version | Author | Date | Changes |
|---|---|---|---|
| 1.0 | M. Crompton | 01/04/2017 | First Draft |
| 1.1 | M. Crompton | 26/10/2017 | Amendments as per the Audit Committee (RE: Email dated 12th October 2017) |
| 1.2 | M. Crompton | 22/11/2017 | Continued amendments as per the Audit Committee (RE: Email dated 12th October 2017) |

## Context

Good robust backup procedures are vital to ensure continuity of services in the event of a system failure or accidental deletion. Across JTMAT Schools we employ a backup strategy that it fit for purpose and provides a robust platform in which to restore systems and/or work.

This policy aims to provide all members of the JTMAT community (staff and students alike) with a detailed understanding of the backup procedures employed and what is/is not backed up.

## Scope of Policy

Any reference to 'the employer' refers to John Taylor Multi-Academy Trust. The 'appropriate level of authority' should be determined according to the employer's decision making structure. This policy applies to employees, visitors and students of the organisation whom have access to the network.

The policy and procedure applies to JTMAT IT Services and all partner organisations, but does not form part of any contract and can be varied from time to time and in consultation with the appropriate bodies.

## What is backed up?

Staff and students have a variety of locations on which files can be stored, it is important to understand which areas are routinely backed up and which are not.

### By JTMAT IT Services

IT Services ensure centrally held data such as PSFinancials and associated information; file, scanned documents and database are backed up on a regular schedule. This does not include the remote access mechanism used by some or partner schools/academies.

### By each School/Academy

Each school will ensure the following areas at a minimum are backed up (if appropriate);

- Staff Shared Area (usually seen as the T drive)
- Student Shared Area (usually seen as the W drive)
- Public Drives
- Web servers including any associated databases, configuration and files
- SIMS.net including any associated databases, configuration and files
- User Document Storage (usually seen as the N drive)
- Specific servers holding the following roles*:

| | | |
|---|---|---|
| Domain Controllers (DC) | Internet Information Servers (IIS) | Database Servers (SQL/MySQL) |
| Domain Name Services (DNS) | DirSync (O365) | PS Financials |
| Dynamic Host Configuration Protocol (DHCP) | Deployment Services (SCCM) | |

*This list is by no means exhaustive and it is expected each school/academy to back up enough data to ensure a full network restore could be initiated if required.

**What is not backed up?**
The following areas and/or devices are not backed up by IT Services and it is the individual's responsibility to ensure adequate secure backups are taken;

- Office 365 Content; including but not limited to OneDrive, OneNote, SharePoint, Email, Calendars and Contacts. Office 365 has its own data recovery systems in place, please see the "Restoring Data Policy"
- Google Contents; including but not limited to Drive, Teams, Sites, Keep, Email, Calendars and Contacts.
- Removable Media
- Memory Sticks or External Hard Disks
- Camera media including SD Cards
- iPad or Android Devices, including any apps or files stored on them
- Future Digital's Policy Central – data for this service is stored offsite in a remote data centre
- Staff laptops unless files are saved to the Documents folder for shared drives
- Apple MAC Devices

If you are unsure if an area is backed up by your local academy please contact IT Services to discuss your concerns and/or an appropriate backup strategy.

## Responsibilities

A good robust backup procedure is vital to ensure the continuity of services in the event of a partial or full systems failure therefore it is important to define the responsibilities of each person or organisation involved.

**The Trust**
The enforcement of the policy lies with John Taylor Multi-Academy Trust although it has chosen to discharge this responsibly to the Strategic Network Manager.

**Strategic Network Manager**
The Strategic Network Manager is responsible for ensuring this policy is implemented and adhered to across each of JTMATs partner organisations including nominating an individual at each site to monitor the backup strategy and report any issues accordingly.

The Strategic Network Manager is also responsible for devising and updating a Disaster Recovery Plan to ensure continuity of service in the event of a systems failure.

**Named Individuals**
Named individuals (see below) are responsible for the day to day management and implementation of the back policy, they provide a single point of contact for issues relating to backup and restoration of services/files.

| Organisation Name | Backup Monitoring | Off-Site Backups |
|---|---|---|
| **John Taylor Multi-Academy Trust** | Andrew Dickson | Andrew Dickson |
| **John Taylor High School** | Alistair Duncan | Alistair Duncan |
| **Kingsmead School** | Andrew Brookes | Andrew Brookes |
| **John Taylor Free School** | Andrew Dickson | Alistair Duncan |
| **Primary Schools** | Office/School/Other third party/Business Manager | |

The above are responsible for the following areas:

- Reporting any issues with the backup strategy or job to the Strategic Network Manager
- Feeding back any improvements to the backup strategy to the Strategic Network Manager
- Recording backups, media used and retention period

- Swapping media as and when required
- Passing backups to the person responsible for Off-Site storage, recording this appropriately to comply with Data Protection (DPA) and General Data Protection Regulation (GDPR) Acts.
- Routinely testing the backup media to ensure they contain valid backups and recoding this appropriately

*Please see Appendix 1 for sample documentation and recording sheets.

**JTMAT IT Services**
JTMAT IT Services are responsible for backing up core financial information and any other services deemed by the Strategic Network Manager to be of core value to the Trust.

**Partner Organisations**
Each partner organisation is responsible for the following:

- Reviewing the Backup Policy and ensuring the named individual is compliant
- Providing a safe and secure storage location for backup media away from the backup device, including the provision of a fire proof safe rated for at least 90 minutes
- Providing the off-site storage personnel with appropriate storage e.g. a lockable safe. If multiple organisations use the same named individual for off-site storage this cost/responsibility could be shared

**Staff/Students**
Staff and students are responsible for backing up any files that are stored in areas that are not backed up (see above list). If you require any help in deciding a backup schedule or how to create a backup, please contact IT Services.

It is advised that any backup taken should not be keep on the same medium or in the same location as the files you have backed up.

**Schedule – Partner Organisations**
Due to an ever-decreasing backup window different types of backups are run on different days. Any files that are modified during the backup windows described below may not be backed up until the next scheduled backup. All backup following the structure below apart from PS Financials data which is backup on a separate schedule.

**Monday-Thursday (Weekly)**
Due to the large amounts of data generated daily it is impossible to create full backup daily, therefor JTMAT has implemented a process of incremental backups during the working week. This process involves backing up files that have changed since the last backup whether that be full or incremental. Combining this type of backup with a full backup ensure we have a robust backup strategy should a system fail.

**Friday (Weekly)**
A full backup is taken every Friday starting at various times depending on the individual organisations requirements of all the files stored in the locations described above. This backup run over the weekend and can take up to 72 hours to complete.

During this time, the availability of the websites and SIMS may vary as the services are stopped to ensure that all files are backed up.

This backup is then transferred to an encrypted tape which is then stored securely off-site by the nominated person.

The tapes are reused after 4-5 weeks and any files contained are overwritten with a new backup.

**School Holidays**
During some holidays (for example for the summer) the backup schedule may be suspended as the number of files being modified or changed is minimal.

**Monthly**
A full backup is taken on the last Friday of every month starting at starting at various times depending on the individual organisations requirements of all the files stored in the locations described above. This backup run over the weekend and can take up to 72 hours to complete.

This backup is then transferred to an encrypted tape which is then stored securely on-site for a maximum of 12 months.

**Yearly (July)**
A full backup is taken at the end of every academic year to ensure that files for staff and student that have left is backed up and can be retrieved on request. No user files will be deleted before this backup has taken place.

This final full backup (Friday) of the academic year will be stored within each organisation and will be retained indefinitely from 2017.

## Schedule – PS Financials

Due to the critical nature of PS Financials across the Trust, JTMAT IT Services has employed a different backup schedule to ensure data loss in the event of partial or full system failure would be minimal.

**Daily (Monday – Thursday)**
A full backup is taken every day (Monday-Friday) starting at 6pm of all the files stored in the following locations:

- John Taylor High School – SQL Server (PS Financials Database)
- John Taylor High School – PSF Server (Electronic copies of documents and configuration information)

This backup is then transferred to an encrypted tape which is then stored securely off-site by the nominated person.

The tapes are reused after 9 days and any files contained are overwritten with a new backup.

PS Financial data is also stored in the appropriate backups as descripted above "Schedule – Partner Organisations" ensuring the data is safeguarded.

## Testing/Auditing

Ensuring a backup is valid is an important step in the backup process and will be conducted once a month at each of our partner organisations following this procedure:

1. A text file on the root of all servers will be created titled "Backup Test" and will contain the following line of information "This is a file used to test the restore function of external media sets"
2. Once a monthly backup has completed successfully, this set will be used
3. Using a minimum of 3 servers the file located on the root must be deleted
4. Restoring from the media taken off site (usually tape), the files deleted in the previous step must be restored and opened to check contents
5. Complete the documentation as required (see appendix 1)
6. Any issues must be reported to the Strategic Network Manager immediately due to the potential impact should a partial or full system failure occur.

## Appendix 1 - Example Documentation

### Backup Log Record

| DATE | Tape Set Name | RETENTION | Tapes Used | NOTES | Location |
|---|---|---|---|---|---|
| Monday, July 1, 2013 | | For Ever | 6649-1, 6645-2 | CC4 Curric EOY 2013 | Safe |
| Monday, July 1, 2013 | | For Ever | 6659-1 | Admin EOY 2013 (July) | Safe |
| Thursday, May 7, 2015 | | For Ever | 6667-1 | CC4 Old Teaching Staff | Safe |
| Thursday, July 9, 2015 | | For Ever | 6640-1 | CC4 Staff/Student Archive | Safe |
| Sunday, October 18, 2015 | | For Ever | 6647, 0888, 6642 | CC4 Backup - Pre Transfer | Safe |
| Saturday, October 24, 2015 | | For Ever | 6672, 6677, 6679 | Final CC4 Backup (Backup Exec) | Safe |
| Wednesday, July 13, 2016 | EOY 2016 | For Ever | 6681, 6682, 6684, 6683, 6685 | Complete no errors | Safe |
| Saturday, November 26, 2016 | MONTH 3 | 3 months | 0886-1, 0887-2, 6646-3, 6655-4 | Complete no errors | Safe |
| Saturday, December 17, 2016 | EOT (Autumn) | 1 Year | 0889, 6643, 6671, 6676 | Complete no errors | Safe |
| Saturday, January 21, 2017 | MONTH 1 | 3 months | 6670, 6675, 6678, 6686 | Complete no errors | Safe |

### PSF Log

**Tapes Used by Date**

| Tapes Used | DATE | Notes | Retention | Location |
|---|---|---|---|---|
| PSF - Monday 1 | 20 March 2017 | Complete no errors | 2 Weeks | Offsite (A.Duncan) |
| PSF - Tuesday 1 | 21 March 2017 | Complete no errors | 2 Weeks | Safe |
| PSF - Wednesday 1 | 22 March 2017 | Complete no errors | 2 Weeks | Safe |
| PSF - Thursday 1 | 23 March 2017 | Complete no errors | 2 Weeks | Safe |
| PSF - Monday 2 | 27 March 2017 | Complete no errors | 2 Weeks | Safe |
| PSF - Tuesday 2 | 28 March 2017 | Complete no errors | 2 Weeks | Safe |
| PSF - Wednesday 2 | 29 March 2017 | Complete no errors | 2 Weeks | Safe |
| PSF - Thursday 2 | 16 March 2017 | Complete no errors | 2 weeks | Safe |

### External Backup Test

[Continued on next page]

# Test Restore Log

In order to conduct this test please follow the procedure below:

1. Identify a minimum of 3 but maximum of 6 servers and record below
2. Browse to the root of each server and delete the following file “Backup Test”
3. Restore using external media (usually tape) the files you have just deleted
4. Confirm you can open and read the contents of each file
5. If successful upload to the JTMAT IT Service Portal
6. If any of the test are unsuccessful upload to the JTMAT IT Services Portal and notify the Strategic Network Manager immediately.

## Organisation Details

| | |
|---|---|
| **Organisation Name** | |
| **Date of Test** | |
| **Person Conducting Test** | |

## Backup Set Details

| | |
|---|---|
| **Date of Backup Set** | |
| **Name of Backup Set** | |

## Server Details

| Server Name | Success | Failure | Notes |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | |
|---|---|
| **Strategic Network Manager Notified?** | |