

**Backup Essentials**

Version 2.0

|  |  |
| --- | --- |
| **Last Reviewed** | March 2024 |
| **Reviewed By (Name)** | Becca de Ville |
| **Job Role** | Service Manager – Cyber Security |
| **Next Review Date** | March 2025 |
| **Version released Spring 2024** | Reviewed and updated in light of DfE Digital Standards |

This document will be reviewed annually and sooner when significant changes are made to the law.

This document is to be understood as guidance and advice only, and is meant to be read in conjunction with NCSC Backup Guidance and the advice of school IT Support staff.

NCSC Backup Guidance is given here: [Offline backups in an online world - NCSC.GOV.UK](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)

CONTENTS

Contents

[1.1 Introduction 3](#_Toc162513872)

[1.2 What do I need to backup? 3](#_Toc162513873)

[1.3 Backups need to be routine, tested and a priority! 4](#_Toc162513874)

[1.4 Backup Storage 4](#_Toc162513875)

[1.5 Back Up Verification 4](#_Toc162513876)

[1.6 Restoring and testing your back up 5](#_Toc162513877)

# 1.1 Introduction

Think about how much you rely on the data you hold, such as student details, emergency contacts, medical information, and administrative information such as quotes, orders, and bank details.

Now imagine how long you would be able to operate without them.

All schools, regardless of size, are advised to take regular, full backups of their data so that they can recover from a cyber security or business continuity incident. A backup may also be a condition of your school’s cyber insurance cover to aid in the recovery of your school’s services, you will need to refer to your insurance documents for further advice on this.

# 1.2 What do I need to backup?

The following table gives you a list of the kinds of information that you will want to back up. This list is not exhaustive, and you may want to add to it with sources identified as part of your business continuity planning and your Cyber Incident Response Plan. When thinking about your school’s critical data, think about where it is stored and how often it needs to be backed up. Some data doesn’t change very much over the school year, but other data such as your MIS may change on a daily basis.

|  |  |  |
| --- | --- | --- |
| **School Process** | **Where is the data stored? Is it onsite, or is it cloud based?** | **How often should it be backed up?** |
| Safeguarding System |  |  |
| School MIS |  |  |
| Cloud Services |  |  |
| Health and Safety System |  |  |
| Email |  |  |
| Curriculum Files |  |  |
| Teaching Staff Devices |  |  |
| Administration Files |  |  |
| Finance / Purchasing |  |  |
| HR / Personnel Records |  |  |
| Asset Inventory |  |  |
| Facilities Management / Bookings |  |  |
| Website |  |  |
| USBs / portable drives |  |  |

Speak to your IT supplier about your Microsoft 365 or Google Workspace set up, particularly email backup to ensure that there are sufficient backups in place. The responsibility for Microsoft 365 data backups lies with the school, and you should determine whether your school could function without access to that data.

# 1.3 Backups need to be routine, tested, and a priority!

Ensure that any backup provides enough of a gap for you to identify an issue and recognise the need to restore. For example, if you backup every other day but don’t know there is an issue for three days the backup will be of limited use.

# 1.4 Backup Storage

As part of the [Department for Education’s Cyber Standards for School and Colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges), it is best practice to ‘have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site.’ This may look like 2 backups of your teaching files taken at different times, stored on a server, then a backup of your server stored on the cloud.

You may not have a physical server onsite, and therefore may be protected from local cyber incidents, but it is still recommended that you have an offline backup following [NCSC 321 guidance](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world). You may also want to check that the following is in place:

* Where you have a cloud-based off-site backup you should check with your IT supplier that it is protected with MFA.
* Permissions to this account are kept to minimum.
* Where cloud services allow it, set up controls to only allow authorised devices to create or append backups.
* Cloud services should deny connection requests when backups are not in use.
* Removable back up media should be secured with encryption.
* If data is secured within a cloud backup solution it must be ‘disconnected’ from other production services to protect from malicious activity. The term ‘digitally disconnected’ refers to the ability to block connections to the backups to protect the data and apply controls to ensure that only the correct personnel have access.
* Check a Data Protection Impact Assessment (DPIA) has been done for each system that stores personal data.

# 1.5 Back Up Verification

Backup verification is the process used to test backups. A manual restore is the only way to fully test a backup and testing should take place regularly to ensure you have data to restore from when it is needed.

If you have difficulty in restoring your whole backup due to resource and time constraints, restore selected files or tables. Whilst this would not be able to fully validate the accuracy of the backup, it may provide a level of reassurance.

# 1.6 Restoring and testing your back up

Testing a backup means you need to test the entire recovery process to make sure you can test your processes and disaster recovery planning and enable staff to understand their roles and the part they should play.

You may also need to consider how you might restore your backup to a different location if your school has to close. You should consider how data might be accessed from a different environment.