#

**Backup Advice**

**(Compiled with reference to National Cyber Security Centre)**

 Version 2.0

**Contents**

[1. Backing up Data 1](#_Toc76376709)

[2. Identifying what data you need to back up 1](#_Toc76376710)

[3. Backups need to be routine, scheduled, and a priority 1](#_Toc76376711)

[4. Backup storage 2](#_Toc76376712)

[5. Consider using cloud-based systems. 2](#_Toc76376713)

[6. Backup Verification 2](#_Toc76376714)

[7. Restore Simulation 3](#_Toc76376715)

[8. Backup Verification Tools 3](#_Toc76376716)

# Backing up Data

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, should take regular backups of their important data, and make sure that these backups are recent and can be restored.

Ensure that any backup media rotation provides enough of a gap for you to identify an issue and recognise the need to restore. (If you rotate media every other day but don’t recognise there is an issue for three days the backup will be of limited use.

It is the school’s responsibility under the GDPR to ensure it can still function following the impact of flood, fire, physical damage, hacking, malware, or theft. Furthermore, if you have backups of your data that you can quickly recover, you cannot be blackmailed by ransomware attacks. (This is when data/services are ransomed for money).

# Identifying what data you need to back up

The data / information your school couldn't function without: documents, photos, emails, contacts, and calendars are obvious. What about tracking data or safeguarding information stored within a computerised system? How is this backed up and do you know how to restore it?

# Backups need to be routine, scheduled, and a priority!

The majority of network or cloud storage solutions now allow you to make backups automatically. Using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

Many off-the-shelf backup solutions are easy to set up and are affordable considering the business-critical protection they offer. When choosing a solution, you'll also have to consider how much data you need to back up, and how quickly you need to be able to access the data following any incident.

# Backup storage

Whether it's on a separate drive, separate computer, or removable storage media, access to data backups should be restricted so that they:

* are not accessible by staff.
* are not permanently connected (either physically or over a local network) to the device holding the original copy.
* are not likely to be affected by the same emergency, i.e. fire / flood. For more resilience, you should consider storing your backups in a different location.

Ransomware (and other malware) can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from.

# Consider using cloud-based systems

\*Remember: Any third-party provider (including those offering cloud storage) need to meet the GDPR / DPA 2018, and due diligence assessments should be recorded.

Unless the school runs its own email server, emails are probably already stored 'in the cloud'.

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from the location of the school.

Service providers can supply schools with data storage and web services without the need to invest in expensive hardware. By handing over school IT services to a service provider, you'll benefit from specialist expertise which may not be financially possible otherwise.

# Backup 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 would provide a level of reassurance.

# Restore Simulation

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 backup to a different location if the system is completely down. You should consider how data might be accessed from a different environment.

# Backup Verification Tools

You can use backup utility tools or third-party backup verification tools to check key points from your backup, such as:

* **Size check** uses a size range and the file size is25 checked against this range. A File size deviation tool then identifies files which do not meet the size check.
* **File integrity check** makes sure that files have not been damaged when being transferred from the source to the backup destination.
* **Archive verification** looks for file corruption before and during the backup process.