Backup For Education: The View From The DfE

What the latest guidance from the **Department for Education** and the **National Cyber Security Centre (NCSC)** means for **your school** and the **actions you need to take**.

Latest DfE guidance on backing up and protecting data

In August 2020, the Department for Education and National Cyber Security Centre (NCSC) shared updated guidance with schools following an increasing number of cyber-attacks involving ransomware infecting the education sector. The cyber-attacks appear to be taking advantage of system weaknesses such as unpatched software or poor authentication and "have had a significant impact on the affected education provider's ability to operate effectively and deliver services."

What do you need to do?

The latest guidance implicitly states the actions that all education providers should take to ensure they are protected against the effects of a possible cyber-attack or ransomware infection.

It is vital that all education providers urgently review their existing defences and take the necessary steps to protect their networks from cyber-attacks.

Along with your defences, having the ability to restore systems and recover data from backups is vital. You should ask your IT team or provider to confirm that:

- They are backing up the right data
- The backups are held offline
- They have tested that they can restore services and recover data from the backups

Read the latest advice from the NCSC here

Key definitions

> What does offline mean?

As ransomware attacks have grown to be more sophisticated over the years, onsite backup servers have become targets for cyber-criminals trying to ensure a ransom is paid. An offline backup protects your data in a location that is separate from the network on which your live data sits. If your backup is on the same network as your live data and a ransomware infection takes hold, all data on the network including your backups is susceptible. With our partners Redstor your data is encrypted before it leaves your site and in transit, meaning only you hold the keys to your data. Data will never be read by Redstor's platform meaning that even if an infected file were backed up it could not propagate, giving you the airgap needed between you live and back up data.

> The ability to restore systems and recover data

If you are infected by a ransomware attack then it is likely that all of your data, not just a single files, will be corrupted, it is therefore imperative that you are able to recover all of your data in a timely manner both from an operational standpoint and in line with regulations such as the GDPR.

Many solutions tick the box of offline storage but with bandwidth limitations they can be extremely slow to recover or access vital data.

By utilising Redstor's InstantData™ you can easily restore files, folders and full servers and access data on-demand with streamed access, leaving you safe in the knowledge that you can recover and access your data in the event of a disaster.

How NCI Technologies can help you meet the latest requirements

With our partners Redstor you can easily select all data for protection and utilise Insight and industry-leading reporting to ensure all of the correct data is being backed up.

Data is encrypted before it is sent to Redstor's secure UK data centres, meaning that even if there is a malicious file amongst your data it cannot compromise the platform and utilising InstantData™ users can rapidly test recoveries and access data on-demand.