redstor

Backup for education: The view from the DfE

Latest DfE and NCSC guidance on backing up and protecting data against the threat of ransomware and malware

The Department for Education and National Cyber Security Centre (NCSC) have issued additional guidance for schools following a wave of targeted ransomware attacks throughout 2020, 2021 and continuing into 2022; this update comes following the NCSC's previous guidance following attacks in August and September 2020.

"In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing."

Read the full update from the NCSC here

What do you need to do?

NCSC 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. IT Teams or providers should 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

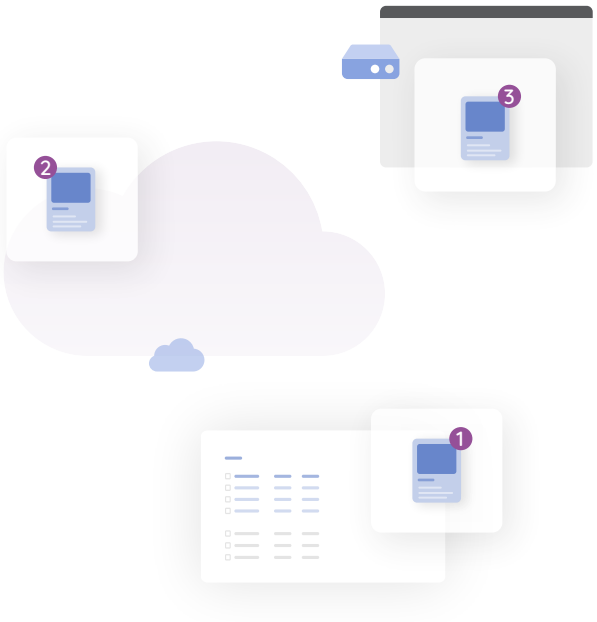
How Redstor helps you meet requirements

Redstor delivers smarter backup and recovery, via an intuitive app, for data residing on infrastructure, cloud-native environments and an ever-widening array of SaaS apps.

Set up in 60 seconds, with zero hardware required, and infused with AI-powered malware detection, Redstor reduces complexity and management overhead, making it the simplest, safest, and smartest way to protect all your data against the ongoing threat of ransomware.

Redstor's proprietary InstantData™ technology enables recovering entire systems in moments, with a seamless user experience that allows users to get back to work almost instantly, streaming what they need, when they need it.

Smarter, DfE compliant backup and protection against ransomware



What are offline backups?

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.

Offline backups are designed with the intention of only being connected to a live network when 'absolutely necessary' and where possible, always having a copy of backup data that is stored separately to the network. This ensures there is always a secure copy of backup data.

With Redstor your data is encrypted before it leaves your site and in transit, meaning only you hold the keys to your data. Even if an infected file were backed up it could not propagate, giving you the airgap needed between your live and backup data.

The ability to restore systems and recover data

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

Redstor's proprietary InstantData™ technology enables recovering entire systems in moments, with a seamless user experience that allows users to get back to work almost instantly, streaming what they need, when they need it.

AI-powered Malware Detection

Redstor's proprietary, AI-powered, malware detection technology neutralizes threats before they become attacks. Scanning all existing backup data, it isolates, quarantines and flags any suspicious files for review, and thanks to community insights, the solution gets better every day.

Ready to try the smartest backup and recovery platform?

Redstor is available through a worldwide network of authorised partners. Speak to your service provider today about Redstor or get in touch with a member of the team at Redstor to get set up with a trial and be put in touch with an authorised partner.

sales@redstor.com | www.redstor.com