

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 and NCSC guidance on protecting data

As of March 2021, the Department for Education and National Cyber Security Centre (NCSC) have issued additional guidance for schools following a wave of targeted ransomware attacks in February 2021.

What data is at risk from ransomware?

LOCAL DATA

Cyber-criminals regularly target data on local servers deemed to be valuable to how a school operates, hoping this will lead to a ransom being paid. This data could be physical, virtualised or even data being synced from cloud platforms. Ultimately, all data is at risk but in recent incidents the NCSC noted that student coursework, school financial records as well as data related to COVID testing had been targeted.



	SaaS	PaaS	IaaS	On-prem
Information and data				
Devices (Mobile & PCs)				
Accounts and Identities				

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

Microsoft Customer

CLOUD DATA

As schools utilise cloud platforms such as M365 and Google Classroom, the data stored in these platforms becomes more important. It is vital therefore that this data is backed up to ensure it can be recovered as and when needed. Contrary to what some believe, the responsibility of protecting this data lies with the user, not the platform providers.

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. These are:

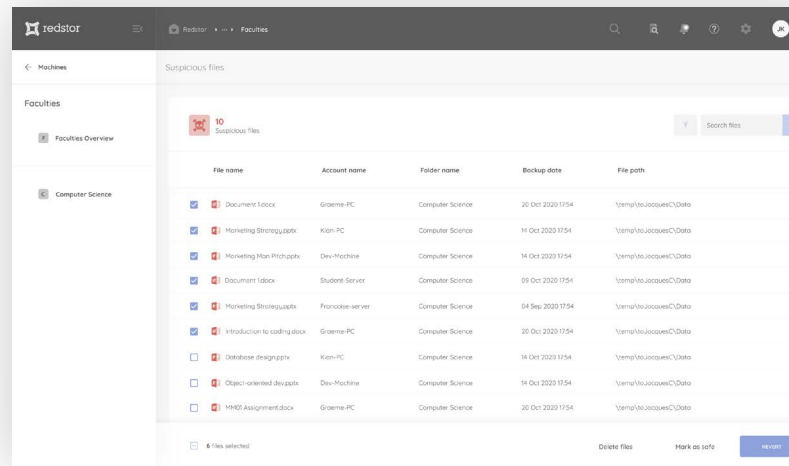
- To confirm they are backing up the **right data**
- Ensuring that backups are held offline
- To test that services can be restored, and data can be recovered from the backups

Read the full advice from the NCSC on mitigating malware and ransomware attacks [here](#)

AI-powered malware detection

As cyber-criminals attempt to hide their activities, the average time taken to detect a malware breach is 206 days. Redstor's malware detection solution utilises AI to enable the detection and removal of malware from within backup data ensuring a clean recovery if one is needed.

Speak to your service provider today to enable malware detection for your backup data.



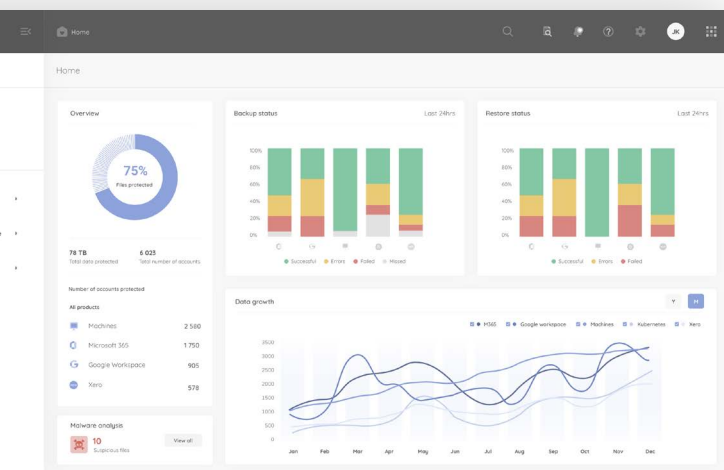
The screenshot shows the Redstor web interface. On the left, there's a sidebar with 'Machines' and 'Faculties' sections. The 'Faculties' section is expanded, showing a list of faculties. The main area displays 'Suspicious Files' with a table of 10 files. The table has columns for File name, Account name, Folder name, Backup date, and File path. The files are listed with checkboxes for selection.

File name	Account name	Folder name	Backup date	File path
Document Table.docx	Grimes-PC	Computer Science	20 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
Marketing Strategy.docx	Kien-PC	Computer Science	14 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
Marketing Plan Pitch.docx	Den-Machine	Computer Science	14 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
Document Table.docx	Student Server	Computer Science	09 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
Marketing Strategy.docx	Francine-server	Computer Science	04 Sep 2020 11:54	\\vamp\fs\locquest\CS\Data
Introduction to coding.docx	Grimes-PC	Computer Science	20 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
Database design.docx	Kien-PC	Computer Science	14 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
Object-oriented design.docx	Den-Machine	Computer Science	14 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data
HW00 Assignment.docx	Grimes-PC	Computer Science	20 Oct 2020 11:54	\\vamp\fs\locquest\CS\Data

How Redstor helps meet your requirements

With Redstor you can easily select all data for protection, whether stored on your local servers or in a cloud platform such as M365 or Google Workspace, 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.



Not using Redstor or having issues testing restores and ensuring you're protecting the right data? Get in touch today to find out how you can start a free two-week trial of the technology.