THE
BUSINESS
RESILIENCE
CENTRE
FOR THE **NORTH EAST**

EDUCATION PACK

INTRODUCTION

A big welcome from our Director, Rebecca Chapman

My name is Rebecca Chapman, I am a Police Superintendent and Director of the North East Business Resilience Centre. Our centre is a home office funded, National Cyber Security Centre endorsed, non-for-profit initiative, which seeks to help organisations become more secure. I am writing to you to discuss the recent circulars which will have reached you from The Department for Education (DfE) and the National Cyber Security Centre warning that cyber criminals were increasingly targeting schools, universities and colleges. These criminals seek to deploy ransomware, depriving educational institutions of their data, subsequently demanding payments to unencrypt the data.
I sincerely hope you never have to deal with such an incident, and that you feel confident that you have the knowledge, tools and resources at your disposal to defend against such attacks. If you don't, fear not we are here to help. We offer low cost, affordable cyber security services which can make a huge difference in your fight against cybercrime. Whether it be training and upskilling of your staff, security testing of your website and networks, or referral into our trusted partner networks to achieve cyber essentials accreditation, we can help. A lot of our advice and guidance is free, and you can receive it by signing up to become a free member of the NEBRC.

What follows is bespoke cyber security guidance, specifically for the education sector, which will give you plenty of food for thought. Please don't hesitate to get in touch with us, if you have any questions.

Very best wishes,

Rebecca

ABOUT US

We are a not for profit organisation working to protect businesses in the North East of England from cybercrime. Our centre brings together all of the North East and Yorkshire's police forces alongside Northumbria University, Sheffield Hallam University and private sector cybercrime experts.

The ethos of the centre is to give businesses access to the latest advice and support from leading police and security industry experts and enable them to learn quick and easy ways to protect their business online. They can meet the "ethical hackers" from our partner universities who can spot the gaps in online security helping to create a safer Humber, Yorkshire and North East for businesses to flourish in.

CYBER SECURITY

An overview

The introduction of the World Wide Web has given criminals the opportunity to target organisations across the globe at the click of a button. However a lot of these attacks can be easily defended against, with the implementation of basic Cyber Security practices.

Cyber Security is how we reduce the risk of cyber attacks, which target our data, reputation and finances. It has three, equal, core components: Technology, Processes and People.

Technology **Processes** **People**

Technology: Using outdated software, having no firewalls, no anti-virus, no encryption and no data backups, mean you are maximising the chances of a successful attack, and limiting your chances of a recovery.

Processes: As Benjamin Franklin once said, "if you fail to plan, you plan to fail", do you have the necessary policies, processes and procedures in place to mitigate cyber risks?

People: You can have the best next generation firewall in the world which protecting your network, but somebody opens an attachment on a phishing email, the firewall has been rendered useless. People are your strongest asset or weakest link. Empower them with knowledge and the confidence to spot these low-level attacks.

There are very few certainties in life, and there is no cyber silver bullet, meaning you can never be 100% certain that your organisation will not be successfully attacked, but you can make compromise less likely. We can help your organisation avoid common cyber-attacks, and help you demonstrate that your company takes cyber security seriously, protecting the data it holds.

NCSC Guidance

Launched in 2016 the National Cyber Security Centre (NCSC) has become the UK's single authoritative voice in Cyber Security. The centre has vast technical expertise and distils this expertise into practical advice which can be used by all organisations and the public. Please find the following free NCSC guidance.

Small Business Guide

A guide containing simple, steps which you can follow to protect yourselves.

https://www.nebrcentre.co.uk/sme

10 Steps to Cyber Security

Guidance designed to help you protect yourself in cyberspace. Breaking down the task of defending your networks, systems and information into their essential components.

https://www.nebrcentre.co.uk/sme

Exercise in a box

A digital online toolkit. It includes two sets of exercises: a technical simulation and table top discussions

https://www.nebrcentre.co.uk/sme

NCSC Guidance continued

Board Toolkit

A range of resources designed to encourage and aid essential cyber security discussions between boards and their technical experts

https://www.nebrcentre.co.uk/sme

Top Tips for Staff

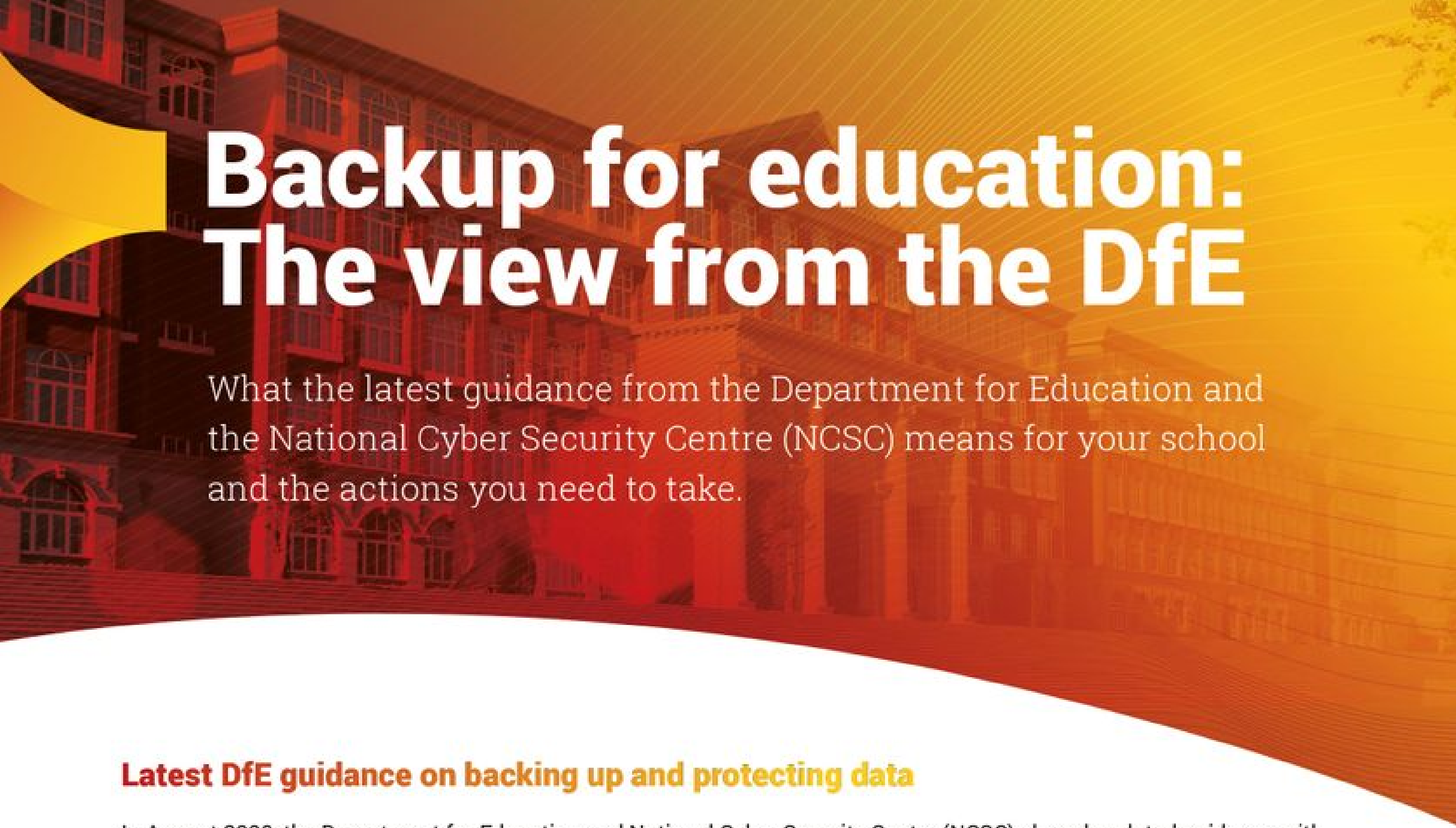
A new e-learning training package, which covers why cyber security is important and how attacks happen. It is totally free, easy to use and takes 30 minutes to complete.

https://www.nebrcentre.co.uk/sme

Cyber aware

Cyber aware is the UK governments advice on how to stay secure online during coronavirus. Many of us are spending more time online, keep yourself and your family secure by following our advice. Stay connected, stay cyber aware.

https://www.nebrcentre.co.uk/sme



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.

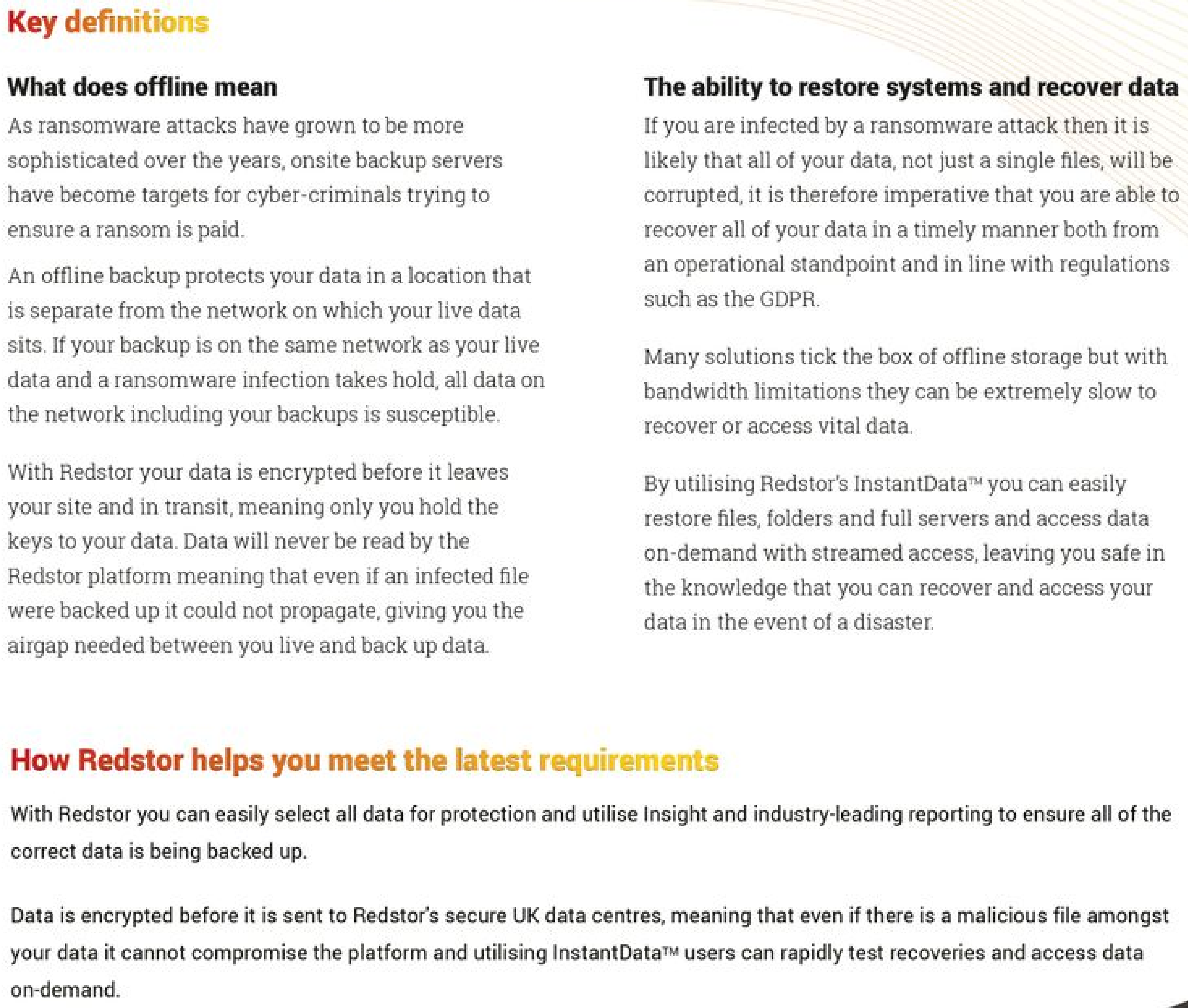
It is vital that all education providers urgently review their existing defences and take the necessary steps to protect their networks from cyber-attacks.

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**

National Partner, of the NEBRC

redstor™



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 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 the Redstor 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 Redstor helps you meet the latest requirements

With 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.

National Partner, Redstor, Haberdashers School case study

ComputerWorld's advice to use Redstor for data protection proved invaluable when only months later a £1 million ransomware attack paralysed Haberdashers' five schools in Monmouth.

Visit this link to know more: https://www.nebrcentre.co.uk/post/national-partner-redstor-haberdashers-school-case-study

redstor
Redstor rescues schools hit by £1m ransomware attack
Data recovery possible thanks to recommendation by ComputerWorld
SERVE AND OBEY
COMPUTER WORLD
Helping Businesses Define Tomorrow™

Useful links

www.nebrcentre.co.uk
A non for profit organisation which helps to support and protect North East businesses from cyber crime.

www.ncsc.gov.uk
The UK's independent authority on cyber security. The NCSC works collaboratively with other law enforcement defence, the UK intelligence and security agencies and international partners. Explore the website for further information, advice and guidance, educational skills and products and services.

www.ncsc.gov.uk/information/report-suspicious-emails
If you have received an email which you are not quite sure about, forward it to the suspicious email reporting service. **report@phishing.gov.uk**

www.ncsc.gov.uk/cyberfirst/overview
Cyber first is a program that provides opportunities to help young people aged 11-17 years explore their passion for tech by introducing them to the fast paced world of cyber security.

www.ncsc.gov.uk/section/keep-up-to-date/cisp
The CISP is the cyber security information sharing partnership, and is a joint industry and government initiative set up to exchange cyber threat and information in real time.

https://www.internetmatters.org/
Internet Matters provide expert support and practical tips to help parents keep their children safe online, while allowing children to benefit from connected technology and the internet.

www.actionfraud.police.uk
Action Fraud is the UK national reporting centre for cyber crime. You can report either online or by calling 0300 123 2040. **NB if you are a business, charity or other organisation which is currently suffering a live cyber attack, please call 0300 123 2040. This service is available 24 hours a day, 7 days a week.**

www.nebrcentre.co.uk

enquiries@nebrcentre.co.uk

NEBRCentre

North East Business Resilience Centre