Cyber-security: Building your school's cyber-defence

Dataspire
Creating ICT confidence for schools

Learn more…
Call: **0345 603 1233** Email: **info@dataspire.co.uk**
Or visit: **www.dataspire.co.uk** for more details

As technology gets smarter, so will the cyber-criminals and the damage they cause can be huge, especially in schools. We've already spoken about the increase in schools being targeted by ransomware and as always, Dataspire is here to help any school that falls victim to cyber-attacks but because "prevention is better than cure", we want to ensure you have all the information at your disposal to proactively shield you and build your school's cyber-defence.

IMPORTANT NOTICE

While the Dataspire team will work with you to build your cyber-defence, it is important to remember it is up to you to ensure cyber-security is given the time and resources needed to secure your school.

Remember: *This is explained in paragraph 131 of Keeping Children Safe in Education (2021)*

"131. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network. In addition, broader guidance on cyber-security including considerations for governors and trustees can be found at NCSC.GOV.UK."

Starting at the beginning

What is Ransomware?

Ransomware is malicious software (malware) that enters your IT system and prevents you from accessing your data or your devices by encrypting it.
Once encrypted, victims are usually held to ransom with threats of disclosure or non-access in exchange for money, and more recently, in Bitcoin or other types of cryptocurrency. Once paid, the victim might be given a decryption code so they can access their data and device or prevent disclosure but as this activity is perpetrated by criminals, there are no guarantees they will even provide a key.

For a school network this can cause even bigger issues as once the ransomware enters the system, it can spread to other devices on the network restricting and ultimately stopping access for all users.

In the early stages, hackers used a scattergun approach targeting anybody and everybody with random messages hoping for success but more recently, they are using more personalised tactics which are likely to have a more connected and emotional response to catch you out. Hackers are also now targeting larger organisations e.g. schools, as opposed to individuals, so that they can demand larger ransoms.

The thing to note is that even if the ransom is paid, there are no guarantees whatsoever that the data will be released. Paying the hackers can also lead to repeat incidents as those victims are often noted as vulnerable and "soft" targets.

Remember: *If you're an academy, you will need to contact the Education and Skills Funding Agency (ESFA) before paying any ransom demands (this is explained in paragraph 6.17 of the Academy Trust Handbook)*

"6.17. Trusts must obtain permission from ESFA to pay any cyber ransom demands. ESFA supports the National Crime Agency's recommendation not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and is likely to result in repeat incidents."

What you can do:

Well, because every school is unique, you may have different systems and services already in place to defend and protect your network but as cyber-crime continues to evolve, prevention isn't as simple as "setting and forgetting" a solution.

Ask yourself these questions:

- **Is your school prepared for a ransomware event?**
- **If your school was to be attacked tomorrow, what would you do?**
- **How do you monitor your network for irregular or malicious activity?**

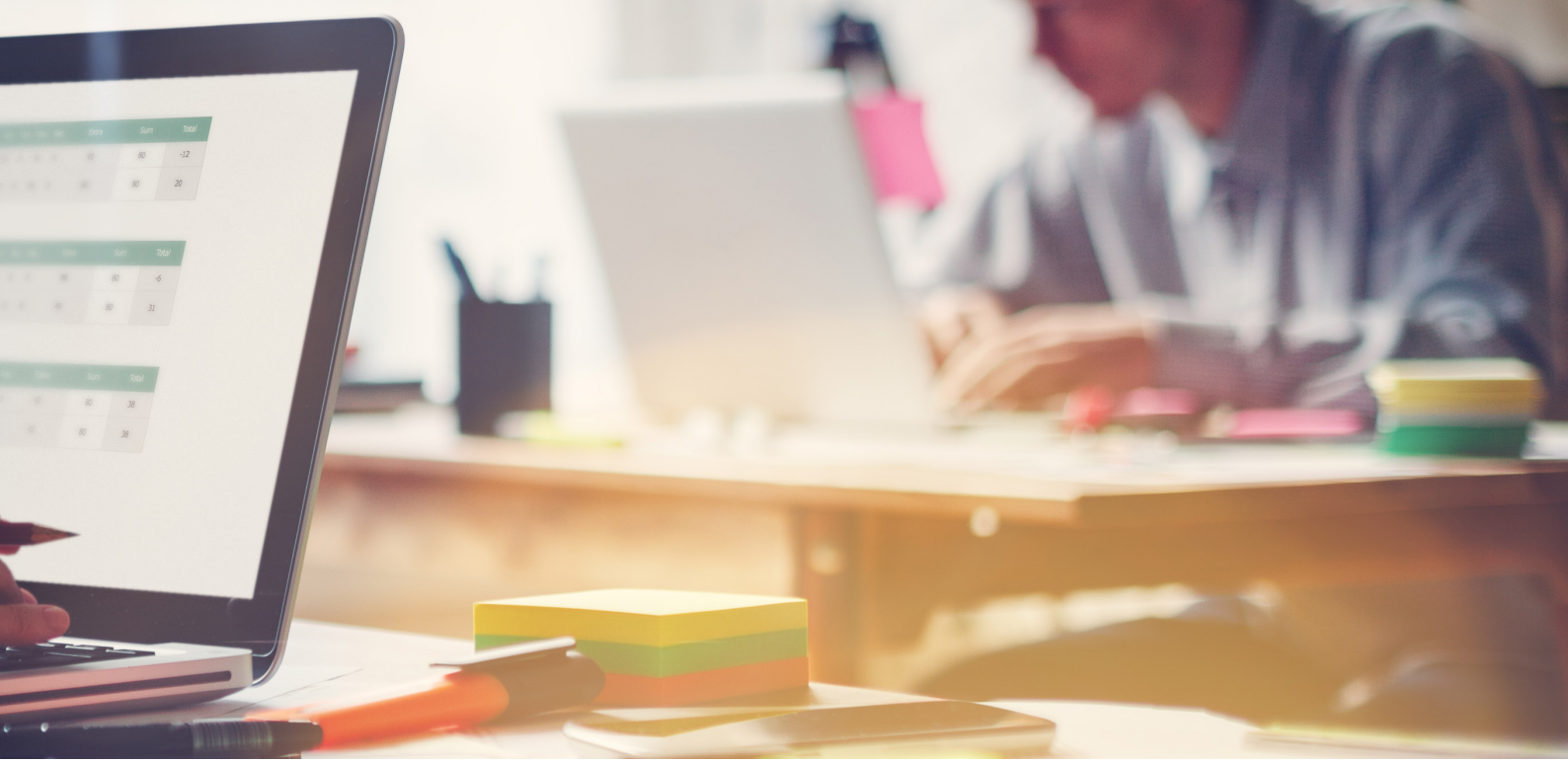
There are some effective steps that schools can take to help protect against cyber-crime, such as:

1) Effective antivirus and security software:

Your antivirus and security software setup should prevent you from malware, ransomware, exploits and viruses. A good antivirus will be able to detect and block both known and unknown malicious software. It should also protect your devices such as desktops, laptops, servers, tablets and mobile devices across all major operating systems. Most antivirus will detect and remove incidents before you encounter them, and will help you to act before the risk becomes too great.

It is important to remember that ransomware operates in a different way to other attacks. It can find its way in through emails initially looking to be from an internal colleague or from a third party with seemingly correct or relevant information asking you to click a link. Once clicked, this will trigger the beginning of ransomware. Your security software needs to look for this specific type of activity and protect you from it. Standard antivirus simply does not look for ransomware activity and thinks of it as normal operation.

Dataspire recommends **Sophos Intercept X** as it is unrivalled in its ability to noiselessly detect and address any ransomware associated activity. Without a doubt, it is the most effective cyber-security protection on the market. **Speak to us for details.**



2) Robust Backup

A good backup solution will protect your data from fire, flood or theft, disk corruption/failure, hardware failure, recover deleted files, recover from failed upgrades and of course, data lost due to ransomware. It will take time to recover as you will usually need to complete a full network recovery, but solid backups will protect your data.

The NCSC recommends the 3-2-1 rule.
Make **3** copies, store them in at least **2** locations, with **1** being offsite. This allows you to be certain that your most important data is safe from incidents.

As a foundation, schools should:

- **Implement a backup solution if you don't already have one.**
- **Decide what data you would like to backup (what data is most important?) and ensure that the backup happens right away. Of course, you can backup as much data as you like but it is crucial that your essential and sensitive data is secured first.**
- **Understand what your backup service provides. For example:**
  - **Are backups restorable and recoverable?**
  - **How quickly can you find and recover the most important data?**
  - **Do your backups return everything that you put in?**

Test your backups. It's all well and good ticking the box to say that you have data backup but when did you last test it? How do you know how easy it will be to action any of the above? The last thing you want to do is wait until an incident to find out, so test your backups and regularly.

Finally, with so many schools implementing the **DfE's offering of a digital education platform**, this data will need backing up too. Shifting to remote learning was challenging enough without having to start from scratch due to data loss. Check that your backup solution can backup Google Workspace for Education and Microsoft 365 too.

The Dataspire Backup solution helps to protect schools' data from cyber-criminals and simple human error. It allows you to access your data completely and immediately, and because it is stored in the cloud, we offer the ultimate security and scalability so that as your data grows, so too will your storage. And yes, this does include your digital education platform. **Speak to us for details.**

3) Staff Training

It's absolutely vital for schools and ALL school staff to understand cyber-risks and how to better protect yourselves online, and by learning how to manage these risks, your school can reduce the chances of being impacted by a cyber-attack.

We've already spoken about how cyber-crime continues to evolve and regular training (annual at least) and updates will provide your colleagues with the tools and skills needed to identify possible risks while keeping them up-to-date on the latest threats and ensure your school data is protected.

Basic safety precautions are your school's first line of defence so please at least remind your colleagues (and regularly) of the following:

- **Check the sender email address, not just the name**
- **Do not click on emails you do not recognise**
- **Be wary of requests for bank details, personal information or login details**
- **Be wary of verifications of requests for payments or changes to information**
- **Check with the sender if an email is asking for data or to click a link that is unusual or just unexpected**
- **Change your password regularly and ensure it is complex**
- **And if something feels strange, it usually is.**

Make sure that you include cyber security training as part of induction for any new starters – this is especially important if they start outside of your school's annual training window.

Remember: This is outlined in paragraph 117 of Keeping Children Safe in Education 2021

"117. Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including online safety (paragraph 114) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 119), that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

It may also be worth noting that paragraphs 123 – 135 provide a new section covering online safety, remote learning, filters and monitoring, information security, cyber-crime, reviewing online safety provision and information and support.

Training and support recommendations:

The National Cyber Security Centre (NCSC) provides free cyber security training for school staff. **Find out more here.** You can download your own **cyber-security information cards** in English and Welsh and send these out to your staff.

Dataspire also works with Go Live Training to provide Online Safety Training.

We can support schools with:

- **An audit of current practice**
- **Online Safety Update for Staff (at least once per year)**
- **Online Safety for Senior Leaders**
- **Online Safety Audit**
- **Online Safety Mark Preparation and / or Assessment**
- **Teaching Online Safety in a Primary School**
- **Teaching Online Safety in a Secondary School**

4) Check what precautions you already have in place

Request an audit

The best way to work out whether what you have in place is working well is to get the specialists in, namely your Dataspire support team. This is because we can objectively test what you have in place, and advise whether it's appropriate for your school.

You shouldn't carry out an audit yourself as you might lack the expertise to determine whether your systems have the right type of security. Plus, as cyber security is a specialised area, it's best looked at by someone who is objective and specially trained. Dataspire has a team of cyber-security trained specialist that can assist you with this. ***Speak to us for details***

In addition to your audit,

- **Dataspire can organise a penetration test (pentest) where we will try to penetrate your network to see how far we can bypass your systems.**

- **Work with you to develop an ICT strategy that will enable you to plan for long-term cyber-security, updating systems, infrastructure and devices to keep you safe.**

You may not want to but it's money well spent. Some elements of making your school cyber-secure can be expensive (for example, replacing your IT software), but the alternative can be far more financially damaging. You may feel that you cannot afford to but can you afford not to?

360 Safe Review

You can also carry out a self-review of your online safety procedures with this **free tool** from 360 degree safe.

These questions/topics are to help you start thinking about what you might need to do to make your school more secure, and can help you spot areas that a formal audit should look at – but it's not a comprehensive list. Be sure to organise a formal audit to identify any gaps in your cyber security.

Is your equipment up-to-date?

Running old, unsupported and out-of-date software can leave your system vulnerable. You need to make sure that your devices and systems are up to scratch and as secure as they can be.

Create an Action Plan

Once you have checked the precautions you have in place, Dataspire can work with you to develop and deliver a cyber-security action plan which will also cover:

- **what procedures you will follow in the event of a cyber-attack,**
- **how you will communicate with your school if communications go down,**
- **who you will contact and when,**
- **and who will notify Action Fraud of the incident.**

You should review and test your procedures with Dataspire:

- **Annually (although ideally every 6 months)**
- **After a significant event has occurred**

In between, you can regularly test your procedures, using the NCSC's **'Exercise in a Box'** to help you practise your response to a cyber-attack. It is completely free and you don't have to be an expert to use it.

It may be a good idea to organise an audit to coincide with the review of your procedures. **Speak to us for details.**

Remember: If you are an academy, the ESFA specifically notes that academies should have 'proportionate controls' in place against cybercrime, which is explained in section 6.16 of the Academy Trust Handbook

"6.16 Academy trusts must also be aware of the risk of cybercrime, put in place proportionate controls and take appropriate action where a cyber security incident has occurred."

The following recommendations are the very basic requirements to ensure schools' cyber-security.

5) Protect your connectivity with a firewall

A Firewall is a network security solution that monitors and filters incoming and outgoing network traffic based on your previously established security policies. Simply put, it's a barrier that sits between your school network and the public Internet. Dataspire provides an education-specific firewall for school internet services ensuring the protection of students, staff and data. **Speak to us for details.**

6) Filtering your Email and Web Activity

When a device attempts to access a web page, the address is checked against a database of URLs. Dataspire's email and web filtering services can help you to analyse, categorise and block all undesirable content. **Speak to us for details.**

7) Network Access Control

Who has access to your network and how much access do they have? Schools should be very specific about who can access their network and at what level. This includes your wireless network as hackers will use all kinds of entry points to attack your system. By knowing (and restricting) access to your network, you can identify irregular activity, e.g. why is that user accessing files or devices that they usually wouldn't?

Ensure you have tight policies restricting privileged access and locking down accounts that shouldn't have unrestricted or unfettered access. Challenge requests for "full domain admin" accounts and confirm exactly what the account needs to be used for and opt instead, for elevated access rather than full privilege.

8) Application (black/white) Listing a.k.a Software Restriction Policies (SRPs):

Application Listing is where you create a policy that only allows/rejects specific apps and programmes being added to your network. This can be put in place to restrict uploads to your network whether online or via external devices such as memory sticks. Ensure applications and services that do not need to be run remotely do not have that capability.

9) Business Continuity Plan:

As with all other processes and policies, schools should make a Business Continuity Plan just in case all the other plans don't work. It's essential to have a plan in place as it's not just about protecting the school from malicious attacks, your Business Continuity Plan provides additional support for internal incidents such as accidental data loss.

All round cyber-security best practice will also help your school in terms of data protection, safeguarding and in more ways than you can imagine as it's all connected.

Why is this important now?

This is even more important now because the NCSC has seen a 300% increase in attacks on organisations and because we know that teaching and learning is becoming increasingly reliant on technology regardless of the subject. It also impacts the daily management of school business operations such as finance and administration, and even communications with colleagues and parents.

By forming good habits now, you can help to prevent your school from issues later down the line and it's not just an issue that should be passed onto your IT support or provision. It needs to be taken seriously by all school personnel as it overlaps with guidance and instruction from Keeping Children Safe in Education and your Prevent Duty.

Cybersecurity is about governance and whole school awareness.

For more support:

Below are all the resources mentioned in this document, plus some additional links, that can be used to make your school more cyber-secure and don't forget to speak with the Dataspire team to discuss what would work best for you.

Resources: *(Click on titles)*

- **Cyber-Security for Schools**
- **Cyber-security information cards**
- **Little Book of Cyber Scams 2.0**
- **Keeping Children Safe in Education 2021**
- **Revised Prevent Guidance: for England and Wales 2021**
- **Academy Trust Handbook 2021**

Tools, training and support

- **Cyber Essentials certification –** this is a government-backed scheme from the NCSC that will help to protect you from the most common cyber-attacks. You can achieve 2 levels of certification. Speak to us for details.
- **Cyber-security training for school staff**
- **360 Safe Review -** Carry out a self-review of your online safety procedures with this free tool

Further reading and references:

- **Cyber Security in education: Is your school safe?**
- **Isle of Wight schools hit by ransomware**
- **Dealing with suspicious emails and text messages**
- **The UKSIC definitions of 'Appropriate Monitoring' have changed**
- **Online safety highlights of Keeping Children Safe in Education 2021**
- **NCSC Alert:** Further targeted ransomware attacks on the UK education sector by cyber criminals
- **DfE to launch cyber-security advice tool after spate of attacks - Schools Week**
- **Offline backups in an online world - NCSC.GOV.UK**
- **National Counter Terrorism: Cyber-security**

Get in Touch!

Visit our website at: **www.dataspire.co.uk**

Email us at: **info@dataspire.co.uk**

Call us at: **0345 603 1233**

Or follow us on any of our social channels:

Whichever way you choose to contact us,

we look forward to hearing from you.