Dataspire

Cybersecurity Guide 2023

Cybersecurity:
Building your school's cyber-defence

With the government reporting a 20% increase in the number of cyber-attacks on education and the average cost of a breach now standing at £10,000, can you afford not to build your cyber-defence?

Year after year, schools and academies are increasingly being targeted and as technology gets smarter, so will the cybercriminals, and the damage they cause can be huge!

With this knowledge comes a wave of new guidelines and expectations to keep your students, staff and data secure so, Dataspire has updated its Cyber Security Guide for 2023/24 with tips and advice that will help you reduce the threat to your establishment.

Cyber Security in Education 2023

The UK government suggests the economic cost of cybercrime to UK citizens is an eye-watering £3.1bn per annum and growing, with the main targets being education, health-care, government and retail, although no company remains unaffected.

But let's focus on education.

To keep students, staff and data secure, the Department for Education (DfE) in partnership with the National Cyber Security Centre (NCSC) has outlined the following guidance:

- DfE Digital and Technology Standards – Cyber Security Standards for Schools and Colleges
- Risk Protection Arrangement (RPA) and eligibility

Cyber Security Standards for Schools and Colleges

Below is a summary of the DfE standards, designed to help schools and colleges protect their data

Protect all devices on every network with a properly configured firewall.

Properly configured firewalls prevent many attacks. They also make scanning for suitable hacking targets much harder.

Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date.

Attackers scan for and exploit devices where the security features are not enabled and recording network devices helps schools keep networks up-to-date and speeds up recovery.

> Backups of important data are crucial for quick recovery in the event of disaster.

Accounts should only have the access they require to perform their role and should be authenticated to access data and services.

If you prevent and limit the compromise of these accounts, you prevent and limit successful cyber-attacks.

You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication.

Multi-factor authentication only allows access to a service when you present 2 or more different forms of authentication. It reduces the possibility of an attacker compromising an account.
This is especially important if an account has sensitive or personal data access.

You should use anti-malware software to protect all devices in the network, including cloud-based networks.

Up-to-date anti-malware and anti-virus software reduce the risk of many forms of cyber-attack.

An administrator should check the security of all applications downloaded onto a network.

Applications can insert malware onto a network or have unintentional security weaknesses. This makes attacks easier to execute against a network.

All online devices and software must be licensed for use and should be patched with the latest security updates.

Unsupported software does not receive security updates and over time it becomes:

- more vulnerable as methods of exploitation are discovered,
- less compatible with the security measures integrated into the network operating system.

> The most common forms of cyber-attack rely on mistakes by staff members to be successful.

You should have at least 3 backup copies of important data, on at least 2 separate devices, and at least 1 must be off-site.

A backup is an additional copy of data, held in a different location, in case the original data is lost or damaged. If all copies were held in the same location, they would all be at risk from natural disasters and criminal damage.

Backups of important data are crucial for quick recovery in the event of disaster.

Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber-attack.

Being unprepared for a cyber-attack can lead to poor decisions, slow recovery and expensive mistakes.
A good response plan made ahead of time will speed up your response, reduce stress levels and confusion.

Serious cyber-attacks should be reported.

This compromise of data might include:

- stealing the data
- copying the data
- tampering with the data
- damaging or disrupting the data, or similar
- unauthorised access

You should report any suspicious cyber incident to Action Fraud on 0300 123 2040 or on the Action Fraud website.

You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by the General Data Protection Regulation

The protection of sensitive and personal data is vital to:

- the safety of staff and students,
- the reputation of schools and colleges,
- the confidence placed in schools and colleges,
- avoid the legal liabilities that security breaches expose schools and colleges to.

Train all staff with access to school IT networks in the basics of cyber security.

The most common forms of cyber-attack rely on mistakes by staff members to be successful. Avoiding these mistakes prevents attacks. Basic cyber security knowledge amongst staff and governors is vital in promoting a more risk-aware school culture.

Backups of important data are crucial for quick recovery in the event of disaster.

To help you meet the standards, Dataspire recommends...

Strategically:

- **You should develop a cyber security policy:** The cyber security policy should outline your approach to cyber security. It should include things like the use of passwords, data protection, and security awareness training.

- **You should conduct a cyber security risk assessment:** The cyber security risk assessment should identify all the potential risks to the school or college's data and systems. It should also assess the likelihood and impact of each risk.

- **You should develop a cyber security incident response plan:** The cyber security incident response plan should outline the steps that will be taken in the event of a cyber-attack. It should include things like how to identify an attack, how to contain the attack, and how to recover from the attack.

- **You should provide cyber security training to staff and students:** Cyber security training should be provided to all staff and students on a regular basis. The training should cover topics such as password security, phishing awareness, and social engineering.

Technically

- **You should use a layered security approach:** A layered security approach involves using a combination of security measures to protect your data and systems. This could include things like firewalls, intrusion detection systems, and anti-virus software.

- **You should keep your software up-to-date:** Software updates often include security patches that can help to protect your data and systems from known vulnerabilities.

- **You should backup your data regularly:** In the event of a cyberattack, it is important to have a backup of your data so that you can restore it quickly.

- **You should test your cyber security measures regularly:** It is important to test your cyber security measures regularly to ensure that they are working as expected.

We can help with all the above, so if you need support for any of these solutions, please contact us at info@Dataspire.co.uk

80000
70000
50000
40000

Risk Protection Arrangement (RPA) and Eligibility

The Risk Protection Arrangement (RPA) is a service set up by the government through which the cost of risks that materialise will be covered by government funds and is an alternative to commercial insurance offered by the DfE.

- If your school is classified as a public sector school, you can join the RPA using your DfE Sign-in account.
- If your school is classified as an academy, you will have been signed up to the RPA automatically, but you can opt-out if you want to.

Cyber Risk Cover through the RPA offers:

£250,000 for any one loss and in any one membership year.

Where a member is part of a group network with other RPA members, the maximum aggregate liability is £750,000 in any one membership year for the group network.

RPA Eligibility

To be eligible for the cyber risk cover, included in the RPA membership, schools and academies must meet and evidence the 4 following security conditions:

1 - All members must meet the DfE's Cyber Security standard relating to backups. Plan to be able to recover and restore your school's data in the event of a cyber-attack.

2 - Complete the NCSC's cyber security training for school staff
Designed for all school staff and governors and earn individual certification.

3 - Register your school with the Police Cyber Alarm tool
This tool detects and provides regular reports of suspicious cyber activity and vulnerabilities.

4 - Implement a cyber response plan
A plan for contingency and recovery in the event of a cyber-attack. The DfE has made a template available on the RPA Risk Management portal.

Dataspire recommends: Schools and academies should implement all DfE/NCSC cyber recommendations to reduce the risk of a cyber-attack.

Modern cybersecurity terms that schools should know...

While the top technique is still phishing, this now takes on several forms to trick users into submitting information.

Phishing, Smishing, Vishing, Quishing, Whaling and Spear-Phishing.

Nope, not a spell from Harry Potter but just a few more modern ways cybercriminals are targeting us. For those of you who aren't already familiar with or aware of the terms, here is a breakdown of what it all means:

(We're confident you know this one.) It's when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link in an email that will download malware or direct you to a dodgy website.

Phishing

Smishing is when scams are sent via text (SMS) messages to mobile phones. Like phishing, you'll receive a message that looks like it came from a trusted source. Display names can be spoofed to make the texts appear authentic.

Smishing

Vishing follows the same thread but this time via voicemail or a phone call. You know, "following your recent accident…" or "you owe HMRC some money…"

Vishing

Since the pandemic, QR codes have made a comeback (touch-free access to information) and because of this, cybercriminals are placing QR codes in places to be clicked and sending you exactly where they want you.

Quishing

Whaling is Phishing for large organisations and the senior executives within - hoping to persuade them into transferring large sums of money.

Whaling

A very targeted form of Phishing that is personalised to you. Whereby, the attacker is disguised as a known and trusted individual.

Spear -Phishing

They all serve the same purpose.

Victims are deceived into giving sensitive information to a disguised attacker and because technology provides a wide range of channels, it also provides a wider range of victims allowing cybercriminals to choose whom they want to target and how.

These attacks are often claiming to be from your bank or Senior Leadership, asking you for personal or financial information such as your account or card number. Providing the information is equivalent to handing thieves the keys to your bank balance.

As more and more people use their personal smartphones for work (BYOD) ph/sm/qu/vishing is no longer just a consumer threat. As the use of mobile devices increases, so too will the cybercrime aimed at these devices.

Here's how it works

Urgency:

Causing a state of panic and urgency is a great distraction as nobody wants to be a let-down and therefore, you will act quickly.

Emotion:

By heightening your emotions, attackers can override critical thinking and drive you into rapid action.

Authority/Trust:

By posing as legitimate individuals and organisations, cybercriminals lower your scepticism. With texts and voice messages being more personal communication channels and QR codes through choice, they naturally lower your defence.

Curiosity:

Using a situation that could be relevant to you personally e.g. finances, online orders etc. allows an attacker to build an effective disguise. The message feels personal, which helps to override any suspicion.

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.

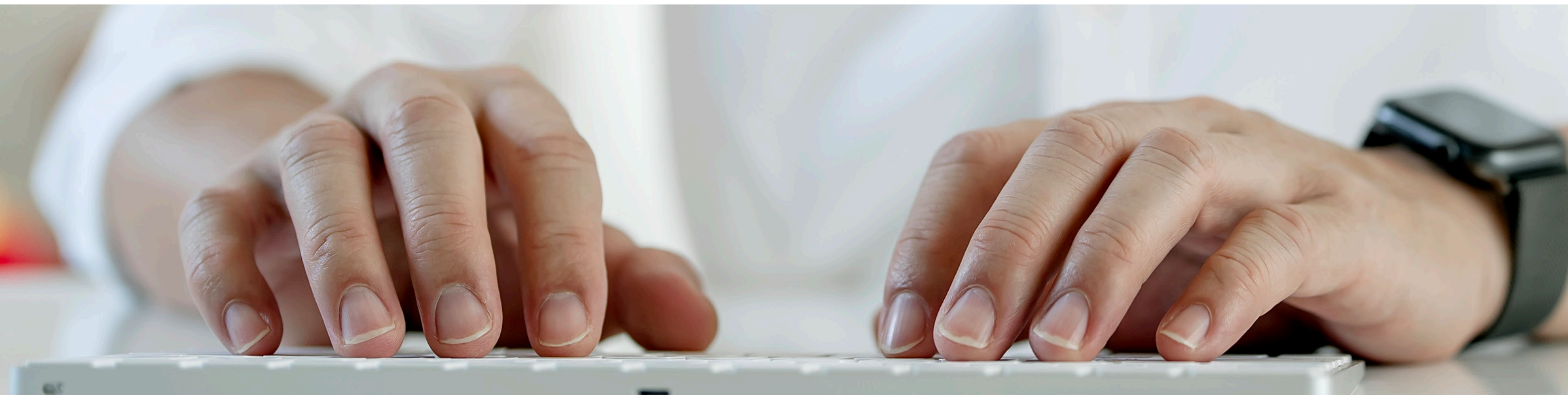
IMPORTANT NOTE:

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 6.15 of the Academy Trust Handbook)

"6.15. 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."



How to reduce the threat of cybercrime in schools

Cybercrime isn't just a technical issue. We are all responsible for keeping our colleagues, students and data safe and secure. While the Dataspire team can 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 144 of Keeping Children Safe in Education
"144. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place 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 Cyber security training for school staff - NCSC.GOV.UK."

Because every school is unique, you may have different systems and services already in place to defend and protect your network, but as cybercrime 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:

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 phishing/ransomware operates in a different way than 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 absolutely 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.

Backup Solutions

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 moving to the cloud, 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.

Dataspire recommends: 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. Learn More.

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 cyberattack.

We've already spoken about how cybercrime continues to evolve and regular training (annual at least) and updates will provide your colleagues (and students) with the tools and skills needed to identify possible risks while keeping them up-to-date on the latest threats to 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 paragraphs 124 and 125 of Keeping Children Safe in Education.

"124. Governing bodies and proprietors should ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners. "125. In addition, all staff should receive regular safeguarding and child protection 32 updates, including online safety (for example, via email, e-bulletins, staff meetings) as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

It may also be worth noting that a definition of cyber-crime can be found on page 145.

Training and support recommendations: The National Cyber Security Centre (NCSC) provides free cyber security training for school staff. You can also download your own cyber security information cards in English and Welsh and send these out to your staff.

Check what precautions you already have in place

Request an audit

The best way to work out whether what you've got in place working well is to get the specialists in, such as 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 specialists that can assist you with this.

In addition to your audit:

Dataspire can organise a penetration/vulnerability test (Pen Test) where we will try to penetrate your network to see how far we can bypass your systems.

We can also 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.

FOR EXAMPLE: Microsoft ended support of Windows Server 2012 and Windows Server 2012 R2 (10 October 2023). These solutions are no longer secure and your school could be at risk if you are still using these systems. Contact us if you need help to upgrade your system.

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:

- Annually (although ideally every 6 months) and
- 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.**

Dataspire can work with you to develop and deliver a cyber-security action plan

REMEMBER:

If you are an academy, the ESFA specifically notes that academies should have 'proportionate controls' in place against cybercrime, which is explained sections 6.9 and 6.14 of the Academy Trust Handbook

"Fraud, theft, irregularity and cybercrime

"6.9 Academy trusts must be aware of the risk of fraud, theft and irregularity and address it by putting in place proportionate controls. Trusts must take appropriate action where fraud, theft or irregularity is suspected or identified."

"6.14 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."

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.

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 analyse, categorise and block all undesirable content.

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.

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 programs to be 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.

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 cybersecurity 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.

Dataspire can help with all mentioned recommendations for Cyber Security so please get in touch - info@dataspire.co.uk

If you think you may have already been attacked...

Where prevention has failed, damage limitation is next to reduce the success of a cyber-attack:

- Report the suspected attack - https://report.ncsc.gov.uk/
- Freeze your accounts to prevent any ongoing attempts
- Change all passwords and account PINs where possible
- Monitor your finances, credit, and various online accounts for strange login locations and other activities.

It's important to be honest when these occurrences take place as they can impact both your personal and professional reputation. Taking these steps (and most importantly reporting the attempt), not only helps you recover but prevents others from falling victim too.

And remember...

Cybercrime isn't just a technical issue. We are all responsible for keeping our colleagues, students and data safe and secure.

Additional 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.

Research:

DfE Cyber Security Standards for schools and colleges

Risk Protection Arrangement (RPA) Membership Rules

Keeping Children Safe in Education 2023

Revised Prevent Guidance: for England and Wales 2023

Academy Trust Handbook 2023

Governance Handbook

DfE Cyber Team Backup Guidance

Little Book of Cyber Scams 2.0

Cyber Security for Schools

Cyber Security information cards

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-attvacks. You can achieve 2 levels of certification.

Cyber Security training for school staff

360 Safe Review - Carry out a self-review of your online safety procedures with this free tool.

Cyber Security Cheat sheet for school staff

Further reading and references:

A Summary: DfE Cyber Security Standards

A Summary: DfE Filtering and Monitoring Standards

A Summary: DfE Wireless Networks Standards

A Summary: DfE Broadband Connectivity Standards

A Summary: Keeping Children Safe in Education 2023

Modern cybersecurity terms that schools should know

Cyber Security in education: Is your school safe?

BBC News Articles: Cyberattacks 2023

The UKSIC definitions of 'Appropriate Monitoring'

Offline backups in an online world - NCSC.GOV.UK

Cybersecurity: the five latest trends,

TechMonitor - September 2023

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.