# YHMAT
# Cyber Prevention Plan

**Adopted February 2023; Last update January 2024**
**Next update January 2025 or with significant change**

## YHMAT undertakes to make cyber security a priority

Cyber security is becoming more important than ever, with many schools falling victim to cyber attacks, particularly ransomware attacks.

### YHMAT will:

- **Ensure that the appropriate level of security protection and procedures in place – see paragraph 144 of Keeping Children Safe in Education (2022)**
- **Keep School data secure**
- **Ensure computer networks are protected.**
- **Train staff in Cyber security**

### Controls that are in place:

- Contracted expert IT company to support the Trust – First Contact Ltd; and two staff members with IT speciality.
- All data is either synchronised with or resides on the NAS Servers.
- The NAS servers are set up with Hybrid Raid arrays so even if one hard drive fails they can continue running and alert IT company
- The NAS servers run multiple daily on site backups to attached USB Storage which is encrypted. In addition they run off site nightly backups to a Synology Data centre in Frankfurt and are also encrypted.
- All user access is limited and restricted the only admin access is either First Contact, R Green or S Rosenhead Trust IT Technicians.
- First Contact proactively check the servers for updates and monitor manufacturer news feeds as well as IT industry sites specifically for warnings of problematic windows updates, more specifically related to the servers.
- All Endpoints – Servers, Laptops, PC's etc are protected with Panda Endpoint Protection Plus.
- Where possible, Staff are encouraged to utilise Multi Factor Authentication when login onto external/cloud based systems.
- Staff Training in Cyber Security Protection is given
- External hard drives and USB's are encrypted with password protection using Windows Bitlocker.

## Future Controls will allow for (to be rolled out in the next 12 months)

- The remote monitor every endpoint for software & driver updates, to automatically update them, to monitor the physical health of the endpoints, such as running temperature, hardware errors etc. this can help avoid hardware malfunction or termination or at the very least allow us to give you advanced notice of potential endpoint failure.
- End User phishing training and testing
- End user password training
- Penetration testing
- Vulnerability scanning

## Action in event of cyber security incident:

**1. Confirm the breach** Contact First Contact/ IT@yhmat.org.uk so that they can identify whether information has been compromised.

**2. Identify the Type of Attack** Whether it's a Virus, Phishing Scam, Malware, Ransomware attack, Spyware or Trojan, identifying what type and location of cyber-attack will help your cyber security specialist(s) with repairing the breach faster.

**3. Contain the Cyber Security Breach** The first step you should take after a data breach is to determine which servers/ devices have been compromised and contain them as quickly as possible to ensure that other servers or devices won't also be infected.

Below are a few immediate things you can do to attempt to contain a data breach.
• Disconnect your internet
• Disable remote access
• Maintain your firewall settings
• Change your passwords
• Install any outstanding security updates or patches

**4. Assess and repair the security breach damage** It's important to assess and repair any breach as quickly as possible. Try to determine the cause of the breach so that you can prevent the same kind of attack from happening again in the future.

**5. Report the Attack** Once the attack has been contained, it's essential to report the incident to Policy Action Fraud. If any data has been breached, then under GDPR businesses are required to contact the Information Commissioner's Office (ICO). Report also to the ESFA especially if a ransom demand made.

**6. Inform any Stakeholders** Staff/parents/suppliers need to be notified, especially if the attack has impacted any data.

**7. Evaluate this plan, review and retrain** Learn from this experience by putting security measures in place to reduce and limit any future cyber-attacks.

**Please also reference our E-Safety and associated Policies.**

**Background and Resources**

**What's ransomware?**

It's a type of malware which stops you accessing your systems and the data held on them - your data could be encrypted, stolen or deleted, and you'll usually receive a ransom note demanding you make a payment to recover the data.

This is one of the biggest threats to schools, but it isn't the only one.

You should also be aware of phishing emails (used to release ransomware via a malicious link or file) as well as the potential for your own students to hack into your network. Get up to speed on various cyber security terms with our glossary.

### It's not just down to your IT department

While you should work closely with your IT department, it's up to you and your governing board to make sure cyber security is given the time and resources needed to make your school secure.

Feel free to share this article with your governors, or if you have The Key for School Governors, direct them to our cyber security content tailored to them.

### 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.

If your school experiences a data breach, its reputation could be damaged and it could be investigated and fined by the Information Commissioner's Office (ICO) – so prevention is definitely better than cure.

## Get support from your LA or trust

You don't need to tackle this all on your own.

Speak to your LA or trust about what it can offer your school regarding cyber security. It may be able to advise you on:

- Different service providers to use (for example, which cyber security auditors to go for)
- Assistance with procurement

### Trust leaders: additional guidance for you

Consider whether:

- You have access to specialised IT support which you could make available to the schools in your trust

- You may be able to get all your schools on the same page through purchasing and updating IT hardware, software and security as 1 trust

# Get training for your staff

This is a crucial part of protecting your school from cyber attacks.

From phishing emails to pressured phone calls, many attacks can succeed as a result of limited staff training.

### Make sure they're trained annually on the basics of cyber security

This is to keep them up-to-date on the latest threats and to refresh their knowledge of what to look out for. Cyber attacks are often spread by email, so basic safety precautions are your school's first line of defence.

Training is particularly important for defending your school against social engineering attacks, such as phishing, and payment fraud. Pages 13-15 of the Metropolitan Police's Little Book of Cyber Scams 2.0 explains that this training should cover how to:

- Check the sender address in an email
- Respond to a request for bank details, personal information or login details
- Verify requests for payments or changes to information

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.

### Trustees and governors can be a target too

Particularly if they're seen to possess valuable information and influence.

This is covered on page 9 of the National Cyber Security Centre's (NCSC's) cyber security toolkit for boards.

**Free sources of training and support:**

- **The National Cyber Security Centre (NCSC)**
  - You can access 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
- Your local **Regional Organised Crime Unit** (ROCU) can work with you to provide free cyber security advice and support so you can improve your awareness of, and defences against, cyber attacks
  - It can also deliver the Cyber Choices programme in your school to help students with cyber skills make the right choices

If you decide to find your own provider to deliver training for your staff, make sure:

- The training is school-specific
- The provider has experience in delivering training to schools

- You're clear on what will be covered in the training – make sure it covers areas such as data as well as phishing and ransomware
- You know what staff should understand by the end of it

# Check what precautions you have in place

The controls your school has in place should be:

**'Proportionate'**

- It's difficult to provide a hard and fast way to tell if what you have in place is 'proportionate', as it'll vary depending on your school size and what tasks people are performing
- The best way to work out whether what you've got in place is proportionate and working well is to get the specialists in, such as through a third-party audit (which we cover further down this article). This is because they will be able to objectively test what you have in place, and advise whether it's up to scratch for your school
- Academies: the ESFA specifically notes that academies should have 'proportionate controls' in place against cybercrime – this is explained on page 58 of the Academy Trust Handbook

**Multi-layered**

- Everyone needs to be aware of cyber security risks – from your front-line staff to your wider supply chain, everyone should be clear on what to look out for to keep your systems safe

**Up-to-date**

- Running old, unsupported and out-of-date software can leave your system vulnerable

**Regularly reviewed and tested**

- You need to make sure that your systems are up to scratch and as secure as they can be

Carry out a self-review of your online safety procedures with this free tool from 360 degree safe.

## Precautions to consider

Below we've listed various areas that you can discuss with your IT manager, IT service provider, LA and/or trust.

Don't treat this as a checklist, self-review or audit. 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.

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.
Staff training
Update your systems and software
Back-up your data
Make sure your management information system (MIS) is secure
Other

# Develop, review and test an incident response plan with your IT department

This should cover what procedures you will follow in the event of a cyber attack.

For example, it should include 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.

Review and test your procedures with your IT department:

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

To test your procedures, use the NCSC's 'Exercise in a Box' to help you practise your response to a cyber attack.

You might decide to organise an audit to coincide with the review of your procedures.

## Trust leaders: additional guidance for you

Your plan should also include the following information for trustees and local governors:

- What their role is during an incident - this is because your chair might be involved with representing your trust in the media
- Who they have delegated authority to
    - For example, who's responsible for escalating concerns, contacting the relevant authorities or taking down your website? (Make sure it includes incidents that happen outside of working hours, too)
- When they want to be informed of the incident. Discuss with them:
    - What significance of incident they want to be notified of
    - What stage during the incident they want to be informed

This is covered on page 35 of the NCSC's cyber security toolkit for boards.

## Organise an annual audit

The best way to know if your school systems are up to scratch is to initiate an annual audit.

Speak to your LA or trust first about a potential provider – they may be able to give you more bespoke guidance.

If it's up to you to pick an auditor, work with your IT manager to choose a third-party provider which:

- Specialises in cyber security
    - For example, if a third-party provider's website advertises lots of different IT services, it might not be a specialist in cyber security
- Has experience in cyber security auditing for schools
    - Schools aren't the same as corporations

An audit should assess what measures your school has in place and where your weaknesses are. It will then identify next steps you can take as a school to tighten up your cyber security.

You can expect an audit to:

- Include a request for your IT department to create your auditor a 'dummy' account which they can use to check your school's security from different levels of user (e.g. to check that as a student user, they can't access anything they shouldn't)
- Conduct a penetration test ('pentest') – the auditor will try to penetrate your network to see how far they can bypass your systems
- Ask to see:
    - An overview of what systems you have in place
    - A risk assessment or incident response plan which covers your school's procedures if there was a cyber attack
    - An ICT strategy plan or similar (for example, if your school improvement plan (SIP) includes that you'll replace your computers, the auditor might ask to see this)
- Give your school some clear next steps to make your network more secure

## Free resources on cyber security

Below we've listed all the resources mentioned in this article, plus some additional links, which you can use to make your school more cyber secure. Work with your IT department to see what would work best for you.**Resources**

- Cyber Security for Schools
- Cyber security information cards
- 10 steps to cyber security (medium and large organisations)
- Small Business Guide: Cyber Security (small organisations)
    - Use the NCSC's checklist of actions you can take
- Little Book of Cyber Scams 2.0

**Tools, training and support**

- Cyber defence tools from the NCSC - find out more about Web Check and Mail Check
- Police Cyberalarm – this is a tool which can help you understand and monitor malicious cyber activity
- Early Warning service from the NCSC – this service will inform your organisation as soon as possible of a potential cyber attack on your network
- 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 – find out more here
- Cyber security training for school staff
- Your local Regional Organised Crime Unit (ROCU) – it can work with you to provide cyber security advice and support so you can improve your awareness of, and defences against, cyber attacks
    - It can also deliver the Cyber Choices programme in your school to help students with cyber skills make the right choices
- Carry out a self-review of your online safety procedures with this free tool from 360 degrees safe

**Resources for trustees and governors**

- Questions for governors and trustees
- NCSC cyber security board toolkit
- Ransomware: what board members should know and what they should be asking their technical experts

# Key terms to understand

**Anti-virus:** software designed to detect, stop and remove malicious software and viruses.

**Breach**: when your data, systems or networks are accessed or changed in a non-authorised way.

**Cloud:** where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.

**Cyber attack:** an attempt to access, damage or disrupt your computer systems, networks or devices maliciously.

**Cyber incident:** where the security of your system or service has been breached.

**Cyber security:** the protection of your devices, services and networks (and the information they contain) from theft or damage.

**Download attack:** where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.

**Firewall:** hardware or software which uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.

**Hacker:** someone with computer skills who uses them to break into computers, systems and networks.

**Malware:** malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.

**Patching:** updating firmware or software to improve security and/or enhance functionality.

**Pentest:** short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

**Pharming:** an attack on your computer network that means users are redirected to the wrong website even if they type in the right website address.

**Phishing:** untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.

**Ransomware:** malicious software that stops you from using your data or systems until you make a payment.

**Social engineering:** manipulating people into giving information or carrying out specific actions that an attacker can use.

**Spear-phishing:** a more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.

**Trojan:** a type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.

**Two-factor/multi-factor authentication:** using 2 or more different components to verify a user's identity.

**Virus:** programs designed to self-replicate and infect legitimate software programs or systems.

**Virtual Private Network (VPN):** an encrypted network which allows remote users to connect securely.

**Whaling:** highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.