SNMAT

Cyber Security Policy

Approved by the Board of Directors – Oct 2022

Policy:	SNMAT Cyber Security Policy
Approved by:	SNMAT Board of Directors
Date:	
Review cycle:	Annual

VERSION CONTROL			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
1	June 2021	D Orridge	New policy
2	August 2022	M Yates	No Changes

Cyber Security Policy

Introduction

1. Cyber-attacks have become more and more frequent in the wake of the recent pandemic and have focused particularly on the education sector. With our strategy of transferring risk to key cloud providers for services such as finance, MIS and child protection we have reduced the chances of a cyber breach considerably. This along with the move to cloud-based file storage in Microsoft 365 and G-Suite the adoption of 2FA have all further reduced the risk of a successful cyber-attack. We must, however, not be complacent as with all systems, we are only as secure as our weakest link. Although we continue to issue guidance to our IT teams and external IT providers to strengthen our security posture against emerging threats, it remains likely we will fall victim to a cyber-attack. Clear guidance, therefore, on how to deal with such incidents and raising awareness of cyber security in general, is essential.

Scope

2. This policy aims to:

   Provide direction and guidance in the event of a cyber incident and encourage staff to report cyber incidents without fear of retribution. The purpose of this document is not to seek out and apportion blame, but to give guidance on how to deal with a potential cyber incident to reduce its impact and to reduce the risk of subsequent attacks.

3. This policy applies to:

   Every member of staff in SNMAT. All staff members have a role to play in cyber security.

Roles and responsibilities

Board of Directors

4. It is the responsibility of the board to ensure there is oversight of cyber security and that the management of cyber security is effective.

Local Governing bodies

5. It is the responsibility of the governing body to ensure there is management of cyber security within the school.

The Principal/Headteacher

6. It is the responsibility of the principal/headteacher to ensure cyber security and the associated cyber incident processes as detailed in Appendices 1 and 2 are enacted and supported in an effective manner.

Staff

7. It is the responsibility of all staff to ensure they understand and can act appropriately to a cyber incident following the guidance laid out in Appendix 1 and following cyber security training guidance.

Trust Support team

8. It is the responsibility of the Trust support team to support and advise the school on the most appropriate actions to remediate a cyber incident and actively advise on and implement security measures and appropriate training as outlined by the NCSC (National Cyber Security Centre) and other cyber security bodies.

Objectives

- To ensure the effects of a cyber-incident are minimised.
- To put in place measures that reduce cyber risk both technical and through staff training.
- To minimise the impact on teaching and learning.

Links with other policies

- ICT Policy
- Bring Your Own Device (BYOD) Policy
- Data Protection Policy
- Social Media Policy
- Policy for Child Protection to Safeguard the Welfare of Children
- E-Safety Policy

Guidance for implementation

9. In the event of a cyber incident the steps outlined in Appendix 1 should be followed by individual members of staff. Once reported, the school should then follow the guidance outlined in Appendix 2 identifying the severity and type of incident.

10. If the incident is identified with a severity of medium or above, the Trust Support Team (TST) IT staff and the local IT support will take over responsibility for remediation of the incident.

11. If necessary and at any point in this process, TST IT staff will act in the best interests of the trust to ensure the CIA (Confidentiality, Integrity and Availability) of the trust's data even if this may conflict with the wishes of the school. Wherever possible, the TST IT staff will liaise with the school, however there may be occasions where swift action is necessary which may disrupt teaching and learning.

12. Incidents identified as high or critical will be reported to the CEO, CFO and trust board as quickly as possible following initial triage and the steps outlined in Appendix 5 will be followed.

Review

13. This policy is reviewed annually by the Trust The application and outcomes of this policy will be monitored to ensure it is working effectively.

Appendices

1 Cyber Incident response - staff guidance
2 Cyber incident response – school guidance
3 Cyber incident severity examples
4 Categorisation of an incident
5 Cyber incident response – MAT guidance

Appendix 1

Cyber Incident response - staff guidance

Introduction

The purpose of this document is to help guide you in the event of experiencing some kind of cyber incident. A cyber incident could be anything from inadvertently clicking on a link in an email and putting in your username and password, to suddenly having all your files encrypted by some malware on your machine.

How do I know if I am the victim of a cyber-attack and what action do I take?

The following are some possible cyberattacks and what to do if you think you have fallen victim to one of them. ***In all cases, please inform the head teacher, IT lead and the business/office manager.***

Signs that your email account has been hacked. Look for the following:

- Your password has changed.
- There's unusual inbox activity (check sent mail, read messages, no incoming emails)
- You have received password reset emails from other sites.
- Your email contacts (whether within or outside of your business) let you know that they have received strange emails from you.

Action:

1. Inform the person in school who can reset your password (there is at least one person who can do this), get them to reset your password.
2. Once you have logged back in with the new password, let IT support know that you think your account has been compromised. They will check to see if any special rules have been put in place by the attacker.
3. Let your contacts know your account may have been compromised and to watch out for strange emails from you.

Signs that your computer may have been compromised:

- Your computer speed has slowed down significantly.
- Your security software has been disabled or compromised.
- Software or browser add-ons appear that you don't recognize.
- Additional pop-ups are happening.
- Random shutdowns and restarts are happening.
- You've lost access to your account.
- Your files become unusable and the icons change.

Action:

1. Shutdown your machine as soon as possible. Do not attempt to retrieve work or email using the machine as it is likely to be infected. Do not attempt to extract files from the device using a USB stick or removable media. Do not attempt to use a removable media device which is plugged into your machine on any other device. The machine needs to be isolated from the network as soon as possible.
2. Inform your IT support or the member of staff responsible for IT in your school. They will reset your password to reduce the risk of further compromise.
3. Give them your machine, do not try and use it again until the device has been checked for malware.

4. IT support will need to check your account and files to ensure malware has not been injected into your local file storage, your OneDrive or any MS Teams/G-Suite classrooms you are a member of. At this stage do not try to log onto the network or Office 365 from any machine.
5. If, after checking with the IT lead, the incident is just confined to your machine and no other files have been compromised, you should now be able to log onto another device with your new password.

Signs your Microsoft 365 storage account (OneDrive or Teams) has been compromised:

- Your site suddenly has content that should not be there.
- You cannot access your account.
- Files are missing/altered.
- You are being notified of unexpected access locations and logins.
- A large number of requests for the same object/file have been received.
- Contacts are receiving emails with files/links to open (make sure they do not open them!)

Action:

1. Inform the person in school who can reset your password (there is at least one person who can do this), get them to reset your password.
2. Once you have logged back in with the new password, let IT support know that you think your account has been compromised. They will check to see if any files have been encrypted or malware applied.
3. Once IT support have checked your account, log in with the new password.

Signs you are the subject of a blackmail demand:

- An email stating that they have incriminating evidence on you (this may or may not be a bluff)
- An email may claim they have accessed your password through a keylogger.
- They threaten to expose you to your contacts.
- They make a demand for payment (most likely in BitCoin)

Action:

1. DO NOT respond to ANY blackmail threats.
2. Inform IT support and your school business/office manager immediately.

Signs your school network has been attacked:

- Your files and/or server has been encrypted.
- Network becomes very sluggish/slow.
- Your data usage is unusually high.
- Programs are continually crashing.
- You received a ransomware message.
- Computers are functioning without local input.

Action:

1. Inform IT support as soon as possible and other staff as soon as possible, it may be affecting them.

Signs of fraudulent financial transactions:

- Money has been transferred to the wrong account.

- Account deductions that you didn't authorize.
- Suspiciously large orders that don't match usual order activity.
- Unexpected invoices that have not been verified.
- Large payments not arriving despite remuneration advice.
- Advice to change address or bank details without the appropriate cross-checks.

Action:

1. Do not pass on any school or financial information.
2. Inform the Trust support team (finance and IT), the headteacher and the business/office manager.

Signs of a malware attack:

- Excessively slow computer processing
- Programs opening and closing automatically.
- Lack of storage space
- New programs/add-ons that you did not install.
- Security software disabled.
- Excessive popups
- Browser keeps redirecting sites.

Action:

1. Shutdown your machine as soon as possible. Do not attempt to retrieve work or email using the machine as it is likely to be infected. Do not attempt to extract files from the device using a USB stick or removable media. Do not attempt to use a removable media device which is plugged into your machine on any other device. The machine needs to be isolated from the network as soon as possible.
2. Inform your IT support or the member of staff responsible for IT in your school. They will reset your password to reduce the risk of further compromise.
3. Give them your machine, do not try and use it again until the device has been checked for malware.
4. IT support will need to check your account and files to ensure malware has not been injected into your local file storage, your OneDrive or any MS Teams/G-Suite classrooms you are a member of. At this stage do not try to log onto the network or Office 365 from any machine.
5. If, after checking with the IT lead, the incident is just confined to your machine and no other files have been compromised, you should now be able to log onto another device with your new password.

Signs of a fraudulent phone call:

- You're being offered money or a free product that you didn't enter to win (reminder: if it seems too good to be true, it usually is!)
- Any call that claims to have detected viruses or infections on your computer.
- Calls that claim you owe taxes or other government payments.
- If the caller deflects or refuses to answer your questions.
- The caller is pushing you to make an immediate financial decision.
- The caller is threatening arrest.

Action:

1. Put the phone down and end the call.

The document in the link below helps explain why cyber criminals are targeting schools and explains some of the terms used in Cyber security. It also gives some tips on how to improve your Cyber security generally.

NCSC and NEN staff support document

Appendix 2

Cyber incident response – school guidance

1. **Identification and initial remediation -** Member of staff identifies a potential cyber breach or attack and takes remedial action. See **Appendix 1** for details of incident types and staff actions.
2. **Response -** Staff member informs the IT lead, head teacher and/or business/office manager.
3. **Assessment -** Initial checks should be made by the school to see if other areas of the school network or Microsoft 365 have been compromised using the guidance above. The guidance in **Appendix 3** should be used as a basis for assessing the level of severity of the incident (Critical, High, Medium, Low). If any indication of the type of incident can be gleaned (using ***Appendix 4***) that will help improve the speed of response and help improve the quality of action that may need to be taken.
4. **Escalation -** School contacts their IT support and the Trust support team if they feel the type and severity of the attack warrants this (ie **the severity is medium or above**). They should pass on what they believe to be the ***severity*** and ***type*** of cyber incident with as much detail as possible. Schools should have their IT support and Trust support team contact details readily available for key staff. Incidents with a low severity should be recorded in a spreadsheet and passed to the Trust Operations Manager on a termly basis.
5. **Isolation -** If the school believe other areas of the network have been affected, then all other devices on the network should be shut down and taken off the network until IT support or a member of the TST can advise on what action to be taken.
6. **Continuity -** Relevant measures should be put in place to allow for continuity with regards to teaching and learning, safeguarding, communications and student information. Have a list of people who you may need to inform in the event of a severe breach eg parents, the ICO etc. You may need to manage the media, discuss this with the Trust Support Team.
7. **Recovery –** Depending on the severity and nature of the attack this may be as little as a couple of hours or may last a week or more.
8. **Mitigation -** The Trust Technical lead and/or the IT Director will come on site to assess the scope of the attack and compile a report (lessons learnt) on the breach and recommend any necessary remedial work that need to be undertaken to ensure the confidentiality, integrity and availability of the school and Trust's data.

Please note, it may be necessary for IT support to take services off-line without consultation if it is felt that CIA (Confidentiality, Integrity and Availability) of data or safeguarding is in any way compromised.

Following an incident, it is worth reviewing the above process to see if it needs to be changed to improve your and the MAT's response.

Appendix 3

Cyber incident severity examples

Severity	Examples
Critical	• Over 80% of staff (or several critical staff/teams) unable to work. • Critical systems offline with no known resolution • High risk to / definite breach of sensitive client or personal data • Financial impact of £[TBC] • Severe reputational damage - likely to impact business long term
High	• 50% of staff unable to work. • Risk of breach of personal or sensitive data • Non-critical systems affected, or critical systems affected with known (quick) resolution. • Financial impact of £[TBC] • Potential serious reputational damage
Medium	• 20% of staff unable to work. • Possible breach of small amounts of non-sensitive data • Low risk to reputation • Small number of non-critical systems affected with known resolutions
Low	• Minimal, if any, impact • One or two non-sensitive / non-critical machines affected. • <10% of non-critical staff affected temporarily (short term)

Appendix 4

Categorisation of an incident

You should also determine what type of incident you are facing. Some examples include:

- **Malicious code:** Malware infection on the network, including ransomware.
- **Denial of Service:** Typically, a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
- **Phishing:** Emails attempting to convince someone to trust a link/attachment.
- **Unauthorised Access:** Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account.
- **Insider:** Malicious or accidental action by an employee causing a security incident.
- **Data breach:** Lost/stolen devices or hard copy documents, unauthorised access, or extraction of data from the network (usually linked with some of the above).
- **Targeted attack:** An attack specifically targeted at the school - usually by a sophisticated attacker (often encompassing several of the above categories).

Appendix 5

Cyber incident response – MAT guidance

Schools follow the guidance outlined in Appendix 1 and Appendix 2

Incidents classified as low severity are recorded by the school in a spreadsheet and sent to the Trust Operations Manager on a termly basis.

At the point of escalation by the school, TST IT staff investigate the incident and confirm its severity and type.

Incidents classified as medium severity are recorded by the TST IT staff in a spreadsheet and sent to the Trust Operations Manager on a termly basis.

If an incident is considered to be high or critical, TST IT staff inform the CEO, CFO and Trust board about the incident as soon as possible, outlining the scope, necessary remedial actions that need to be taken and probable timeframes for recovery. TST IT staff go on site, alongside local IT support to work on restoring services and maintain communications with the CEO, CFO and trust board through the Trust Operations Manager (TOM).

TST IT support and local IT support staff will enact, if required, local and/or cloud-based recovery procedures (DR plan) to restore the necessary services.

CTO, CFO and TOM work with the school to manage media, continuity (including communications, telephony etc) and any other operational issues that may arise. The TST IT staff will advise on any requirements to inform ICO if there have been any data breaches.

Once the remediation is complete a report will be compiled and submitted to the trust board outlining the nature and scope of the breach and detailing what subsequent actions need to be taken to reduce the risk of such an event occurring again. This will be submitted at the next scheduled meeting alongside a summary of low and medium severity incidents or more immediately if deemed necessary.