Valour MAT Cyber Attack Response Plan

Contents

Introduction

This policy outlines the procedures and responsibilities for responding to a cyber attack affecting Valour MAT, and its two primary schools, Walbottle Village Primary School and Beech Hill Primary School. As the hosting and security infrastructure is managed by the ICT Services of Newcastle City Council, collaboration with this department is crucial in any response to a cyber attack. The aim of this policy is to minimise disruption, protect data, and ensure the safety of the Trust's IT systems. This policy applies to all staff, students, contractors, and third-party vendors working with or for the Trust. It addresses the steps to be taken in the event of a cyber attack on the MAT's IT systems or network.

Examples of potential cyber attacks

Below is a list of examples of some of the forms that a cyber attack on an academy / primary school could take.

1. Phishing Attacks

A staff member, such as the business manager, might receive a seemingly legitimate email from a known contact or supplier. The email contains a link to a malicious website that mimics a trusted service (e.g., a bank or payment portal). Once they log in, the attackers gain access to their credentials. This can lead to unauthorised access to sensitive financial information or payment systems.

2. Ransomware Attack

Cyber criminals could send malware to encrypt the school's data (e.g., student records, payroll information, or lesson plans). The attackers demand a ransom payment in exchange for decrypting the files. This type of attack can disrupt teaching, communication, and administrative functions until the system is restored.

3. Hacking Administrative Accounts

If a hacker gains access to the business manager's account or the headteacher's email, they can manipulate sensitive financial or operational systems. This could involve redirecting funds, tampering with payroll details, or sending fraudulent emails to other staff or parents requesting payments for fake services.

4. Data Breach

A data breach could occur if hackers gain access to the school's network and steal personal data, including staff details, student medical records, or contact information for parents. This can lead to identity theft or exploitation, putting both staff and students at risk. In the event of a data breach or suspected data breach, we would refer to our GDPR protocols.

5. Distributed Denial of Service (DDoS) Attack

A DDoS attack overwhelms the school's internet services by flooding the network with excessive traffic. This can take down key services like email, virtual learning platforms, and access to shared resources, causing significant disruption to online learning and communication.

6. Social Engineering

Attackers may impersonate senior leaders or external authorities (like the local council) in order to trick staff into revealing sensitive information. For instance, an attacker might call the IT technician, pretending to be from the ICT Services of Newcastle City Council, asking for login details to "resolve an issue."

7. Wi-Fi Network Compromise

If the school's Wi-Fi network is not properly secured, attackers could infiltrate it to intercept sensitive communications or gain access to connected devices. This could allow them to steal login credentials, manipulate classroom resources, or access confidential data.

8. Malware on Shared Devices

Shared computers, laptops, or tablets could become infected with malware, especially if students or staff unknowingly download malicious files from untrusted sources. Once installed, the malware could spy on users, steal credentials, or further infect the school's network.

9. Credential Stuffing

If staff members reuse passwords across multiple platforms, attackers could exploit stolen login details from another breached service to access the school's systems. This method often leads to unauthorised access to email accounts, cloud services, or finance systems.

10. Unauthorised Access via Third-Party Software

Primary schools often use third-party applications for education, administration, or communication (e.g., student management systems, virtual learning platforms). If these services have weak security measures or aren't regularly updated, they could be a backdoor for hackers to gain access to school systems.

Roles and Responsibilities

1. Cyber Incident Response Team (CIRT)

In the event of a cyber attack, the following people will be part of the response team:

CEO of the MAT or Designated Senior Leader: Primary decision-maker for school operations, including communication with the Newcastle ICT Service and parents.

ICT Service of Newcastle City Council: Responsible for identifying, containing, and mitigating the cyber attack. They will lead technical investigations and recovery efforts.

School ICT Coordinator: Acts as a liaison between the schools and the Newcastle City Council ICT Service, ensuring prompt communication.

Data Protection Officer (DPO): Responsible for ensuring GDPR compliance, handling data breaches, and communicating with the Information Commissioner's Office (ICO) when necessary.

Cyber Attack Response Plan

1. Detection and Identification

Alert Notification: The MAT, along with ICT Services of Newcastle City Council are responsible for detecting potential cyber attacks, such as phishing, malware, ransomware, or denial-of-service (DoS) attacks. Any member of the Trust's staff or students who detects suspicious activity must report it immediately to a member of the **CIRT***,* who will then report the incident to Newcastle City Council ICT Service.

Initial Investigation: Newcastle City Council ICT Services will investigate the reported incident to determine the nature and scope of the attack.

2. Containment

Short-term Containment: The ICT Services will isolate affected systems to prevent further spread, including disconnecting the school's network from external systems if necessary.

User Access Suspension: If compromised, access to IT systems (e.g., email, shared drives) will be suspended for all users within the Trust until it is safe to resume operations.

Communication to Staff and Students: The MAT will send out initial communication to all users, informing them of the potential breach and providing instructions on how to proceed (e.g., logging off devices, avoiding suspicious emails).

3. Eradication

Malware Removal and Patch Deployment: Newcastle City Council ICT Service will work to remove any malicious software and apply necessary patches to secure the network.

Root Cause Analysis: The ICT Service will determine the cause of the attack, whether it was a result of human error (e.g., phishing) or technical vulnerability (e.g., outdated software), to help prevent a further incident from occurring again.

4. Recovery

System Restoration: Once the threat has been contained, the ICT Service will begin restoring systems from backups (if necessary) and bringing the affected systems back online.

Testing and Verification: All restored systems will undergo thorough testing to ensure there are no remaining vulnerabilities before resuming normal operations.

-Password Resets: If the attack involved compromised credentials, all affected users will be required to reset their passwords.

5. Communication and Reporting

Internal Communication: Regular updates will be provided to the Trust's leadership team, staff, and students during and after the incident.

External Communication: The Trust's CEO or Designated Senior Leader, with guidance from the DPO and Newcastle ICT Services, will be responsible for communicating with parents and other external stakeholders if necessary.

Regulatory Reporting: If the cyber attack involves a data breach, the DPO will report the incident to the ICO within 72 hours of discovery, as required under GDPR.

6. Post-Incident Review

Incident Debrief: After recovery, the CIRT will meet to review the incident, assess the effectiveness of the response, and identify areas for improvement. The MAT may revise its cybersecurity policies, conduct additional training, or implement new security controls.

7. No cast-iron guarantee

It should be noted by the Mat's stakeholders, that while the ICT Services at Newcastle City Council is committed to going "above and beyond" to protect its customers, there is no cast-iron guarantee that all cyber attacks can be stopped.

Third-Party Vendors

Many schools use third-party platforms for administration, communication, or teaching purposes, and if these platforms are compromised, they can become an entry point for cyber attackers. Here are some examples of how this might occur:

1. Compromised Educational Software or Website

If a third-party educational platform (e.g., for virtual learning) is hacked, attackers could potentially access sensitive information. For example, if the platform stores student data, attendance records, or progress reports, a breach could expose this data to unauthorised parties.

2. Supply Chain Attacks

A supply chain attack occurs when attackers target a third-party vendor with access to the school's systems. If the vendor is compromised, attackers may be able to exploit their software or service to gain access to the school's network. For example, a compromised software update from a trusted vendor could include malware, which is then installed on the school's network when the update is applied.

3. Data Breach at the Vendor

If a third-party service provider experiences a data breach, any personal data the school has shared with that vendor could be exposed. This might include student names, addresses, medical information, or staff payroll details. The breach could lead to identity theft, fraud, or further targeted attacks on the school.

4. Insecure Integrations

Schools often use multiple digital tools that integrate with one another, such as student management systems, online learning platforms, or communication tools. If one of these integrations is insecure or poorly managed, it could create a vulnerability that attackers can exploit to gain access to other connected systems within the school.

5. Phishing or Social Engineering via Third-Party Platforms

Attackers could use a compromised third-party platform to distribute phishing emails or malicious links to school staff or students. For instance, if a learning platform used by the school is hacked, the attackers might send fake communications (impersonating the platform) to trick users into revealing passwords or clicking on malicious links.

6. Third-Party Cloud Storage Vulnerabilities

Many educational websites and platforms store data in the cloud. If the cloud provider used by the third-party service is compromised or doesn't have adequate security measures in place, attackers could gain access to sensitive school data. This risk is heightened if the service provider doesn't encrypt data properly or fails to secure access controls.

7. Outdated or Vulnerable Software

Some third-party providers may fail to keep their systems updated with the latest security patches. If the software or platform that the school has bought into has vulnerabilities due to outdated code or poor security practices, attackers could exploit these weaknesses to gain access to the school's data or network.

8. Preventative Measures for Schools

To reduce the risk of a cyber attack stemming from third-party platforms, schools can take the following precautions:

Vendor Risk Assessment: Conduct thorough evaluations of third-party providers before entering into agreements, ensuring they follow strong cybersecurity practices. Advice can be sought from our IT security partners at Newcastle Civic Centre if there are concerns about the safety of using a particular third-party provider.

Data Protection Agreements: Ensure that data-sharing agreements with third-party providers comply with data protection laws such as GDPR, and clearly outline the vendor's responsibilities in case of a breach.

Monitor Software Updates: Regularly check for updates from third-party vendors and ensure that security patches are applied promptly.

Limit Access to Data: Only share the minimum necessary data with third-party vendors, and ensure that sensitive data is encrypted.

Staff Training: Educate staff on the risks associated with third-party platforms and phishing schemes related to these services.

Teaching in the event of a cyber attack

If there is a period of time in which our school's IT systems are shut down, teachers will revert to non digital learning. In the event that the outage continues into the following days, access to saved resources on the schools' drives such as lesson planning, presentations, and digital resources such as White Rose Maths could be unavailable for a period of time and so teachers must adapt their lessons and resources. Teachers must also be prepared to plan non-digital lessons for the subsequent days to come in the event of continued unavailability of IT services.

Newcastle City Council's ICT Services Overview

Newcastle City Council's ICT Services provides the functions and activities to support and maintain the school's management and administration system. In summary, this includes the following:

- Service Desk support
- Server support for installations of SIMS.
- Server management and administration, including access control
- SIMS server software installation and upgrades
- Data backup and recovery
- Remote account administration and user support
- Administration of users, including adding and removing of users and groups and setting up access permissions
- Assisting users with support calls
- Support for the SIMS system also includes:
- Software usage advice
- Implementation support
- Documentation and user guides
- Web-based links to Exam boards including results download service
- Support and advice in respect of school management and administration systems, including strategic planning, design of technical solutions and project management for technical implementations.

Terms and conditions of the Service

Terms and Conditions which apply to these Services are detailed in the document - Terms and Conditions for the Provision of Services to Schools and Academies in Newcastle 2023-2024.

Commencement and Duration

The Service Level Agreement (SLA) will commence on the 1st April of each calendar year for 12 months. The SLA will remain in force until either party gives the required notice specified in the standard terms and conditions to terminate this contract. The service and pricing will be reviewed annually.

Backup and Recovery

To minimise the risk of data loss in the event of system failure, an appropriate backup solution will be implemented by ICT Services. Regular maintenance checks will be made to ensure the integrity of the backup solution. In the event of system failure, a full restore will be performed, providing the school has carried out appropriate backup procedures (for local servers).

Problem Management

Requests for service received by the ICT Service Desk are logged onto the incident management system. Each incident is assigned a priority according to the nature of the request. Once the incident is logged onto the system it will be subject to automated prioritisation and escalation procedures. System failures will be given priority over all other activities. Each incident will be given a priority and responded to in the time-scales shown. Due to the nature of ICT problems, resolution times cannot be guaranteed and will be dependent on the nature of the fault.

Security

Security is a key component of effective ICT Systems and it is fundamental to the successful delivery of the services provided that the roles of the school and ICT Services are clearly understood.

Responsibilities of ICT Services

ICT Services will perform the necessary functions and activities to ensure the security of physical devices and data stored on the ICT infrastructure in terms of both the school local area network and the schools broadband network. In summary this includes the following:

Network Security

The includes management of user accounts and permissions to files, applications and networked data, and the management of the security of network devices, e.g. firewall, network switches etc.

Data Backup

In order to minimise loss of data in the event of a system failure, an appropriate backup solution is implemented on application and file servers resident on the central broadband network and the local school network. Regular maintenance checks will be made to ensure the integrity of the backup solution. In the event of system failure, a full restore will be performed, providing the school has carried out appropriate backup procedures (for local servers).

Physical Security

Servers resident on the central broadband network are hosted in server rooms at the Civic Centre. These server rooms are secure (access restricted to designated personnel), fully air conditioned and server racks are equipped with uninterruptible and redundant power supplies. ICT Services recommend that servers located within the school building are stored in lockable areas with restricted access.

System Resilience

All severs resident on the schools' broadband network are configured to provide 24 by 7 services by the use of clustering, redundant hardware and failover facilities. SIMS data is stored on a networked storage system, independent of the file and application servers. In the event of a server failure, the data will still be accessible by alternative server. School based servers have a limited level of resilience, i.e. redundant power supplies and hard disks. In the event of a total server failure, connection to the data will be lost and the server will be swapped out and the data restored from the last successful backup.

Agreed: 1st July 2025

To be reviewed: 1st July 2026

Appendix A: Incident Impact Assessment

Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	
No Impact	There is no noticeable impact on the school's ability to function.
Minor Impact	There is some loss in the ability to function which is minor. Functions can be carried out, but may take longer and there is a loss of efficiency.
Medium Impact	The school has lost the ability to provide some critical services (administration **or** teaching and learning) to **some** users. The loss of functionality is noticeable, but work arounds are possible with planning and additional resource.
High Impact	The school can no longer provide any critical services to users. It is likely the school will close or disruption will be considerable

Informational	
No Breach	No information has been accessed / compromised or lost.
Data Breach	Access or loss of data which is **not** linked to individuals and classed as personal. This may include school action plans, lesson planning, policies and meeting notes.
Personal Data Breach	Sensitive personally identifiable data has been accessed or extracted. Data which may cause 'significant impact' to the person / people concerned requires a report to the ICO within 72 hours.
Integrity Loss	Data, which may include sensitive personal data, has been changed or deleted. (This also includes corruption of data)

Restoration	
Existing Resources	Recovery can be promptly facilitated with the resources which are readily available to the school.
Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
Third Party Services	Recovery is not guaranteed, and outside services are required to facilitate full or partial restoration.
Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.

Appendix B: Communication Templates

1. School Open letter to be copied on Valour / school headed letter format with yellow sections completed as appropriate.

[Date]

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the school IT systems. This means that we currently do not have any access to [telephones / emails / server / MIS etc] At present we have no indication of how long it will take to restore our systems. [OR it is anticipated it may take XXXX to restore these systems]

We are in liaison with our school Data Protection Officer and, if required, this data breach will be reported to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR. Every action has been taken to minimise disruption and data loss.

The school will be working with Newcastle City Council's ICT services and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and normal working as soon as possible. In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff. The school will remain open with the following changes [detail any changes required]

I appreciate that this will cause some problems for parents/carers with regards to school communications and apologise for any inconvenience. We will continue to assess the situation and update parents/carers as necessary. [If possible, inform how you will update i.e. via website/text message]

Yours sincerely,

[name]

2. School Closed letter to be copied on Valour / school headed letter format with yellow sections completed as appropriate.

[Date]

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down the school IT system. This means that we currently do not have any access to [telephones / emails / server / MIS etc]. At present we have no indication of how long it will take to restore our systems.

We are in liaison with our school Data Protection Officer and this data breach has been reported to the Information Commissioners Office (ICO) in line with the requirements of the Data Protection Act 2018 / GDPR. In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff. I feel that we have no option other than to close the school to students on [XXXXXXXXXX]. We are currently planning that the school will be open as normal on [XXXXXXXXXX]

I appreciate that this will cause some problems for parents/carers with regards to childcare arrangements and apologise for any inconvenience but feel that we have no option other than to take this course of action. The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and re-open as soon as possible. We will continue to assess the situation and update parents / carers as necessary. [If possible, inform how you will update i.e. via website / text message].

Yours sincerely,

[name]