Ouston Primary School

Cyber Security Policy

Review Date: Summer Term 2026
Next Review Due - Summer Term 2027
Reviewed by: Full Governing Body

Content

1. Introduction

The purpose of this policy is to highlight to Trustees and all staff of the potential risks of cyber-attacks for the school, making clear what we currently have in place to prevent such events occurring, and to highlight what is regarded as the basic principles of good cyber security.

A cyber-attack is an attack launched from one or more computers against another computer or network of computers. It can maliciously deactivate computers, steal data, or use a compromised computer as a launch point to further aggravate the attack. The two aims of cyber-attacks are to either disable the system or gain illegal access to the target computer or network. There are different types of cyber-attacks based on their specific method and intention.

A cyberattack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually the attacker seeks some type of benefit from disrupting the victim's network.

In the past few years the National Cyber Security Centre has issued a number of alerts to schools, warning of an increase of malware attacks, in particular ransomware, targeting educational establishments. A number of schools have been forced to pay ransomware so that they can recover their data.

The complexity and variety of cyberattacks is ever increasing. While cybersecurity prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks.

In addition to implementing good cybersecurity practices, we are advised to keep systems and security software up to date, leverage firewalls and threat management tools and solutions, install antivirus software across systems, control access and user privileges, backup systems often, and proactively watch for breached systems.

2. Common Types of Cybersecurity Attacks affecting schools

Here are some of the most common types of cyber-attack methods used by cybercriminal gangs around the world.

Phishing

Phishing is a technique used to deceive a target into taking harmful action such as downloading malware disguised as an important document. A targeted phishing attack could be used to gain access to a user's account that has important information (such as a member of the Senior Leadership Team) or a user with administrative privileges to the network.

Phishing is usually in the form of an email sent to either a list of users or targeted at single user. The attacker would craft an email and disguise it to be seemingly normal, with malware attached that looks like it could be a normal document. The email could also include a link that goes to a website designed to look like a familiar website and trick the user into entering their credentials.

To prevent phishing attacks, it is recommended the email system should have an effective filter, implementing email authentication methods like SPF, DKIM, and DMARC to filter potential spam. Users should also be trained on how to identify potential spam emails before clicking on any links or documents attached.

Ransomware

Ransomware encrypts the target files on the system so the user cannot access them. The attacker then demands payment to restore access to the files.

A ransomware attack usually happens when a user opens a malware file or link on a network connected computer. The malware file has specific scripts to identify and encrypt the files in the target area. Ransomware could be used to encrypt a school's financial and contact data so that the school would not be able to access it.

To prevent ransomware attacks, it is a good practice to have On-access scanning enabled on all user devices to scan for viruses before accessing files. Firewalls should be enabled on host devices and anti-virus software should be updated with the latest security patches.

Password attack

Password attack is an attempt to gain access to systems by cracking the user's password. Once the user password is cracked, the attacker can gain access to either confidential data or an administrative account allowing access to all data or make significant changes to the network.

A targeted password attack usually involves the attacker finding out details about the user and then attempting to use that information to determine the correct password.

Passwords are also sold on the dark web by criminal gangs that have been leaked or hacked from organisations. A good practice to follow is not using the same password twice. The use of complex passwords with a mixture of words, numbers, and special characters are strongly advised by cybersecurity experts. Another way of preventing password attack is to enable multi-level authentication on systems that support it.

Brute force

Brute force is an attempt to gain access to systems by trying different passwords to eventually guess the correct one. Similar to a password attack, the attacker could gain access to privileged user accounts. Malware that is installed on the network with direct access to a systems login screen can be used to secretly attempt to guess a user's password.

One of the prevention tactics is to configure locking the accounts. Accounts should lockout if there are too many failed attempts at logging in. Audit logs should also be configured and regularly reviewed by the system administrator for any abnormal use of accounts.

Denial of Service (DDoS)

Sending so much traffic to a computer or network such that its resources are overwhelmed and they are made unavailable to anyone. When affected by a Denial of Service attack, the school would be unable to access and use the affected systems.

An attacker compromises a computer or multiple computers using malware that instructs them to send traffic to a single target. In the case of multiple computers, it is called a distributed denial of service attack. Systems should be built and configured around the concept of redundancy and the ability to fail-over to a secondary system if the first is unavailable. Systems should also be designed with the ability to deal with increased load over the average normal usage.

3. Connected it Solutions – Schools Technical Support

The school has an annual Service Level Agreement with Connected IT Solutions.

The following is a list of measures that the Technical Support Team provides to protect our school network from cyberattacks.

Internet security and filtering

- Firewalls – checking of incoming and outgoing info on the network
- Anti-virus software – detection and removal of viruses and malicious software
- Backups –protection against human error, power failure, natural disasters and virus attacks

4. National Cyber Security – Practical Tips

The National Cyber Security Centre has issued practical tips for everyone working in education. Each school needs to look after its data as well as manage the risks of using networked computers and servers. Cyber security is about protecting the devices we use in school and the services we access on line, both at home and work, from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on the devices and on line.

Cyber Security is important to schools because a number of schools have been seriously impacted by cyber incidents: perhaps a phishing attempt to steal money and passwords, or a ransomware attack that encrypts files preventing access. Many cyber incidents are untargeted and can affect any school that does not have basic levels of protection. As a school we hold lots of sensitive information, for example staff and parents bank details, medical information about students and safeguarding records. All of this has to be kept safe and confidential.

Cyber criminals understand that a school's information is sufficiently important that they might be prepared to pay a ransom to get it back. Potentially Cyberattacks could be undertaken by the following:

- Online Criminals – Good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.
- Hackers –Individuals with varying levels of expertise, often operating in an untargeted way, to disrupt just for the sake of it.
- Malicious Insiders – use the access they have to conduct malicious activity.
- Honest mistakes – sometimes staff will just make an honest mistake.

Powerful Passwords

When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks in school.

Here's how to use them well:

Have a different password for each account / service. If this isn't possible then make sure your most sensitive accounts (e.g. access to student records) have a unique password.

If you must write down your passwords, store them securely and away from your device.

On the advice of the IT team, two factor authentication should be considered in specific circumstances. This gives a way of double-checking you really are who you are claiming to be.

Always lock your account when you step away or stop using your device, even if it's just for a minute. This applies in school or when working from home. A good way of creating a strong and memorable password is to use three random words.

Passwords should be easy for you to remember but hard for somebody else to guess.

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal your details to sell or perhaps to access your organisation's information.

Reducing phishing emails needs to happen at different levels.

'If in doubt, call it out'. Always ask for advice if you're not sure if the link or email is legitimate

If you feel you may have compromised your security, report this to the Head Teacher or the IT team as soon as possible so they can try to minimise any damage.

Watch out for phish! Some phishing emails are more sophisticated than others, but it helps to be aware of some of the more obvious clues. These include:

- Phishing flags Does it contain poor quality images of logos?
- Are there spelling or grammatical errors?
- Does it address you as 'dear friend' rather than by name?
- Is it asking you to act urgently?

- Does it refer to a previous message you don't remember seeing?

5. Summary

Cybercriminals use a variety of methods based on their motive to attack school systems. Schools should have robust IT infrastructure and data protection policies to deter possible cyber-attacks. Following good data protection practices and methods will ensure if ever there is an attempted cyber-attack, the school's assets and intellectual property are secure. It will also ensure the downtime is minimal and the systems are restored at the earliest.

As well as taking the appropriate steps to reduce the impact of any potential Cyber Securities attack all staff will be asked to complete Cyber Security training and to sign an E-safety/acceptable use agreement.
Link to Cyber Training below:
https://www.ncsc.gov.uk/information/cyber-security-training-schools
This tells staff what is acceptable in the use technology and communications (including social media). The school has disciplinary measures in place, should staff not adhere to the guidance.