Cyber Attack – School Entity - Incident Response Plan

INTRODUCTION

Foresight's IT Team are responsible for all client/customer incident response and are committed to managing risk to your schools IT systems, including cyber-attacks or breaches.

The Cyber Attack Incident Response Plan may be needed in response to the following common cyber-attacks:

- **Phishing and spear phishing attacks.** Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing the user;
- **Password attack.** Passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach;
- **Malware attack.** Malicious software can be described as unwanted software that is installed in your system without your consent.
- **Firewall Breach Attack –** Attackers will attempt to gain access to an organization network by breaching the perimeter network.

Any of the above cyber-attacks could directly impact normal day-to-day operations at your school. This plan will anticipate risks to the security of our network and systems, and will provide escalation and action plans, to ensure that your school is ready to deal with cyber-attacks as they occur.

1 SCOPE

This Cyber Attack Incident Response Plan relates to all staff, across all functions

2 PRINCIPLES AND PURPOSE

Through this Cyber Attack Incident Response Plan, the school will:

- Provide guidance on Cyber Attack Incident Response.
- Provide a consistent approach to Cyber Attack Incident Response within the school
- Ensure that all members of staff fully understand their responsibilities and the reporting structure.
- Ensure that all members of staff are aware of, and fully comply with relevant legislation, regulations, codes of practice and school policy, when there are issues with the security of our data.

3 RESPONSIBILITIES

4 Headteacher

Overall accountability for Cyber Attack Incident Response across the school lies with the headteacher, who has responsibility for establishing and maintaining an effective management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5 Business Manager

The Business Manager is accountable to the Headteacher and will be expected to *understand* how the strategic business goals of the school may be impacted by cyber and information risk. The Business Manager will also ensure that risk is mitigated through the development of robust Risk Management Policies and Procedures, Business Continuity and Incident Response Plans. The Business Manager will also be responsible for providing leadership and communication during a cyber-attack.

6 Foresight IT Services

Foresight will support risk management, incident response and business continuity planning, including testing the plan once ratified. Foresight will also ensure that appropriate systems are in place to prevent, detect and analyse cyber-attacks within a reasonable timeframe.

7 Data Protection Officer

The Data Protection Officer is responsible for providing advice and monitoring compliance with Data Protection legislation, and ensuring the organisation is able to meet the Data Security and Protection standards.

8 All Staff (including Volunteers)

Every member of staff and school stake holder must:

- Comply with the requirements of relevant legislation and codes of practice during Cyber Attack Incident Response.
- Comply with the Cyber-Attack Incident Response Plan, including all supporting guidance

Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy/strategy and procedure manuals
- Line manager
- Specific training courses, for example, induction training, e-learning, etc.
- Other communication methods, for example, team meetings

A breach of legislation, codes of practice or any of the School policies/plans could result in disciplinary proceedings, up to and including dismissal and/or prosecution of the school or the individual.

INITIAL RESPONSE TO CYBER-ATTACK

Initial incident response deals with the immediate impact of an incident including plan activation and escalation, ensuring people and the environment are supported wherever possible.

In the event of cyber-attack, the first point of contact should be the Foresight Helpdesk, who will perform initial investigations, contain the incident and escalate the problem to the wider team:

Department / Role	Name	E-mail	Telephone
Foresight - IT	Craig Barratt / Ged Tod / Simon Ball / Taylor Hodgkinson	operations@foresightuk.com	0161 738 1099
Business Manager			
Headteacher			
Data Protection Officer			

The Business Manager will put an incident response meeting into the calendar. If the recovery plan takes longer than a day to execute, a meeting will be held daily to manage arising matters and provide updates regarding the outage to the wider Information Security team. In the absence of the Business Manager, the DPO will act as deputy.

9 BUSINESS CONTINUITY PLANS

The plans below outline the actions that must be taken, should a cyber-attack be detected by any member of staff of volunteer. If cyber-attack has been successful, i.e. the system has been compromised, an incident must be raised in Vantage.

a. Receiving a Suspected Phishing/Malicious Email

If a suspected phishing/malicious email is received, the staff member must not click links, enter credentials or open attachments. The user must *call* Foresight UK immediately and forward the email to operations@foresightuk.com.

Tell-tale signs of phishing or malicious include:

- Unexpected emails, that ask the recipient to do something: click a link, open an attachment, provide details or credentials;
- Urgency – asking the user to respond or take action quickly;
- Authority – the email may look like it comes from a senior or legitimate internal/external individual or organisation;
- Mimicry – the email may look legitimate, for example a SharePoint file from a trusted sender;
- Curiosity – the email may include information about your interests or current projects.

If a user forwards a suspected phishing or malicious email, Foresight wil undertake the following action:

- Check Microsoft 365 Defender Compliance Centre, and run the ‘content search’ for the subject or sender of the suspicious email. If the email has been successfully delivered to

the inbox or spam folder of any user, an email must be sent to them to warn them not to open the email, and to delete it immediately.

- Review the authentication controls to verify that the sender is the true sender of the email. If the address has been spoofed or is an invalid contact, then the domain should be blocked.

b. Successful Phishing Attack - Compromised Credentials

If a user's credentials have been compromised, Foresight must also:

- Reset the password immediately and ensure that Multi Factor Authentication has been enabled for the affected user(s).
- Check the Microsoft 365 Defender Compliance Centre log-in audit log, to identify unauthorised access. This can be done by reviewing the IP address and location of the log in. If any unauthorized logins are found, close the sessions.
- Check the mailbox for unwanted rules. If any are found, the function of the rule must be documented and then deleted from the mailbox.

c. Successful Malware Attack – Malicious Code

If a user has clicked on a malicious link in an email, Foresight must:

- Reset the password immediately and ensure that Multi Factor Authentication has been enabled for the affected user(s).
- Run a scan of the device and the server using relevant Anti Virus.
- Re-image the device to ensure no malware remains on the device.

d. Successful Firewall Breach

If an external user/system has managed to gain access to the schools network via an attempt through the firewall Foresight must

- Power down the firewall immediately
- Run a virus/malware scan on all servers & endpoint devices.
- Power up the firewall - Check event/audit logs on the firewall in a cold state (disconnected from the internet)
- Change the password of the firewall device
- Review all external port access to the network

10 TRAINING

All relevant staff will be made aware of the Cyber Attack Incident Response Plan during onboarding and this plan will be tested annually by the Headteacher.

11 DISSEMINATION AND IMPLEMENTATION PLAN

This Cyber Attack Incident Response Plan will be reviewed by the school Business Manager &/or Headteacher.

12 COMPLIANCE

Compliance against this plan will be monitored by the Business Manager &/or Headteacher.

APPENDIX A: CYBER ATTACK INCIDENT RESPONSE PLAN TEST

The Business Manager or Headteacher will test this plan annually to ensure that it is fit for purpose and ready for implementation.

Auditors & Date:					
No.	BCP Audit Activity	Completed (Y/N)	Issues / Actions	By Who & When?	Status
1	Staff member receives an unwanted phishing email – what action would you take?				
2	Foresight receive Phishing email into the operations@foresightuk.com email account, what action would you take?				
3	A user has clicked a link in an email and has provided their user name and password, what action would you take?				
4	A user has clicked a malicious link in an email, what action would you take?				
Test Signed off by:					