DarBro Computers Ltd
ITS ALL ABOUT THE SERVICE

THIS DOCUMENT CONTAINS SENSITIVE INFORMATION AND SHOULD BE KEPT SECURE AT ALL TIMES.

Security Incident Response Plan

Cheshire Federation

Created By: **Daniel Pretorius**

Reviewed: **06/02/2023**

Contents

Introduction 3

Scope 3

Security Incident Response Team (SIRT) – Contact Information 4

Typical structure of a cyber incident response 6

Triage and Escalation Processes 7

Record Keeping 8

Roles and Responsibilities 8

- Incident Response Lead 8
- Employees (General Staff) 8
- Security Incident Response Team (SIRT) 9

Security Incident Response Checklist 10

Incident Severity and Category Matrix 11

- Incident Severity 11
- Incident Category 12

Examples of Incident Response Processes 13

- Malware (or Malicious Code) 13
- Loss of Equipment 13
- Denial of Service Attack (DoS) 14
- Non-Compliance with our Security Policy 14
- Sustained attack by using multiple vectors 15
- Unauthorised Wireless Access Points 15

Resources for Staff Training 16

Cybersecurity Incident Notification Form 17

Introduction

The purpose of this plan is to provide operational structure, processes and procedures to the relevant staff in the **Cheshire Federation**, so that they can effectively respond to incidents that may impact the function and security of data, information resources, and business operations. This plan will be referred to as the **Security Incident Response Plan** or **SIRP** going forward.

Cyber-attacks can quickly escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Whilst much of the Incident Response will be managed within the IT Security environment, early consideration should be given to engaging both Infrastructure Experts and School Leaders in order that the wider issues can be managed efficiently. Infrastructure Experts and School Leaders in the organisation must therefore be familiar with the SIRP and the processes.

The SIRP will assist the **Cheshire Federation** in identifying, managing, investigating, and remediating various types of cyber incidents. It describes the processes for initiating a response and establishing the structure needed to ensure response execution at an appropriate level. This **SIRP** will also reference procedural documentation that provides operational-level details specific to handling the various incident types. This documentation should be regularly reviewed and updated where necessary to ensure accuracy and reliability of procedures.

The SIRP cannot anticipate and provide guidance for all potential incidents. The **Security Incident Response Team** should consider the current situation, business impact, and security needs of the **Cheshire Federation** and balance those against the guidance and recommendations provided by the **SIRP**.

Scope

The **SIRP** applies to data stored within the Information Systems and Networks of the **Cheshire Federation,** both on-site and off-site (cloud hosted) and any person or device who gains access to these systems or data. This plan must be followed by all personnel including full-time staff, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of the **Cheshire Federation**. For simplicity, all of these personnel are referred to as ‘Staff Members’ within this plan.

Security Incident Response Team (SIRT) – Contact Information

The persons below are the key contacts in the event of a cyber-security incident. Contact details should be reviewed and updated regularly. Primary Contacts make up the main **Security Incident Response Team (SIRT)** with Secondary Contacts being available to assist or step in if deemed necessary or if a Primary Contact is not reachable. The severity of the incident will also determine which members of the SIRT need to be contacted.

Phone calls should be prioritised over e-mails in the event the e-mail system might be compromised.

Primary Contacts

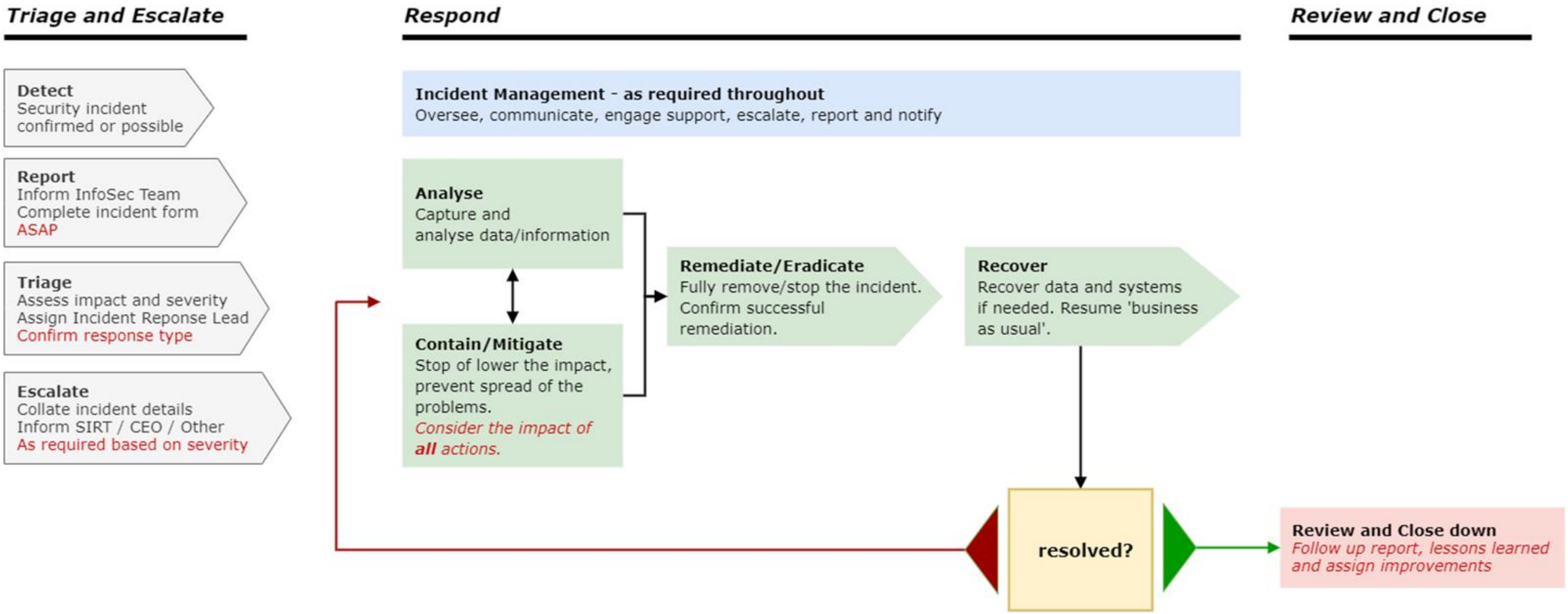
Name	E-Mail	Main Phone	Ext	Mobile
Daniel Pretorius IT Technician/Technical Director DarBro Computers Ltd	daniel@darbro.co.uk / cyberincident@darbro.co.uk	01270 879101		07917430712
Darrin Pretorius Managing Director DarBro Computers Ltd	cyberincident@darbro.co.uk	01270 879101		07900447149
Jackie Irlam Business Manager Cheshire Federation	bursar@gainsborough.cheshire.sch.uk	01270 696810	30304	
Chris Adlington Principal Cledford Primary School	head@cledford.cheshire.sch.uk	01606 663667	10103	
Justine Nurse Principal Cheshire Federation	head@gainsborough.cheshire.sch.uk	01270 696810	30303	

Secondary Contacts

Name	E-Mail	Main Phone	Mobile
Zoe Doyle Finance Officer Cledford Primary School	finance@cledford.cheshire.sch.uk	01606 663667 10116	
Heather Woolley Vice Principal Gainsborough Primary School	hwoolley@gainsborough.cheshire.sch.uk	01270 696810 30302	
Lucy Wagstaff Vice Principal Cledford Primary School	lwagstaff@cledford.cheshire.sch.uk	01606 663667 10102	
Jane Booth Federation Head Teacher	federationhead@gainsborough.cheshire.sch.uk		
Julie Sercombe Chair of Governors	jmsercombe50@gmail.com		

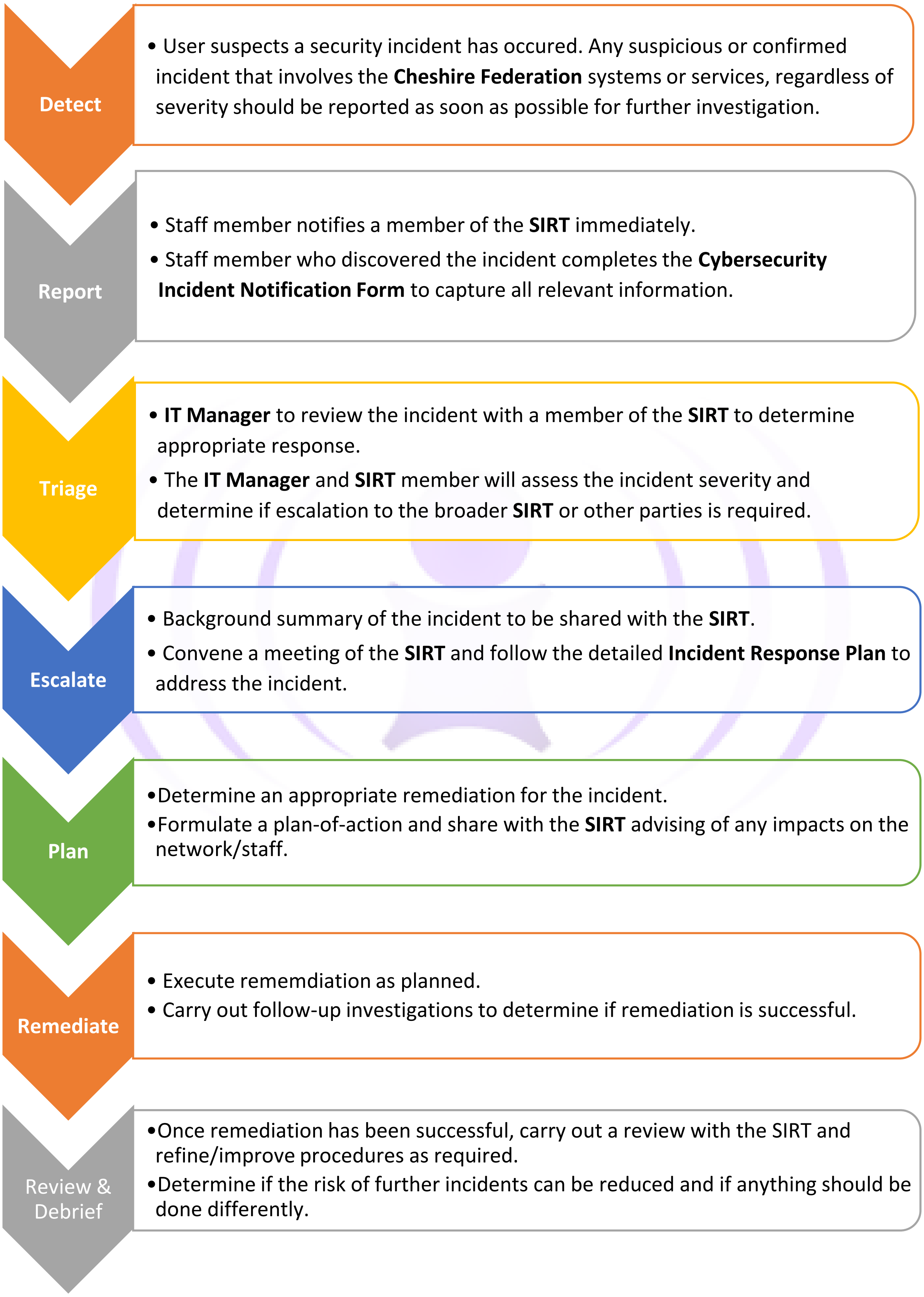
Typical structure of a cyber incident response

The flow charts below outline the general processes that should be followed in the event of a security incident. It serves as a template and guide from the early stages of detecting a confirmed or possible security incident through to remediation, recovery and prevention.



Source: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes

Triage and Escalation Processes



Detect

- User suspects a security incident has occured. Any suspicious or confirmed incident that involves the **Cheshire Federation** systems or services, regardless of severity should be reported as soon as possible for further investigation.

Report

- Staff member notifies a member of the **SIRT** immediately.
- Staff member who discovered the incident completes the **Cybersecurity Incident Notification Form** to capture all relevant information.

Triage

- **IT Manager** to review the incident with a member of the **SIRT** to determine appropriate response.
- The **IT Manager** and **SIRT** member will assess the incident severity and determine if escalation to the broader **SIRT** or other parties is required.

Escalate

- Background summary of the incident to be shared with the **SIRT**.
- Convene a meeting of the **SIRT** and follow the detailed **Incident Response Plan** to address the incident.

Plan

- Determine an appropriate remediation for the incident.
- Formulate a plan-of-action and share with the **SIRT** advising of any impacts on the network/staff.

Remediate

- Execute rememdiation as planned.
- Carry out follow-up investigations to determine if remediation is successful.

Review & Debrief

- Once remediation has been successful, carry out a review with the SIRT and refine/improve procedures as required.
- Determine if the risk of further incidents can be reduced and if anything should be done differently.

Record Keeping

Records and documents created by the **SIRT** should be saved in the **Cyber-Security** folder under the SLT drive. Summary notes and background information for each incident will be maintained in the **Cheshire Federation Cyber-Incident Register**. There should be digital copies and paper copies of these records stored securely.

Roles and Responsibilities

Incident Response Lead

- Making sure that the **Security Incident Response Plan (SIRP)** and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
- Making sure that the **SIRP** is up to date, reviewed and tested, at least once each year.
- Making sure that employees with **SIRP** responsibilities are aware of their responsibilities.
- Leading the investigation of a suspected breach or reported security incident and initiating the **Data Breach Response Plan** (in accordance with the GDPR), as and when needed.
- Reporting to and liaising with external parties, including service providers, legal representation, law enforcement, etc. as is required.
- Authorising on-site investigations by appropriate law enforcement or forensic personnel, as required during any security incident investigation. This includes authorising access to/removal of evidence from site.

Employees (General Staff)

- Making sure they understand how to identify and report a suspected or actual security incident.
- Immediately reporting a suspected or actual security incident to a member of the **IT Team**.
- Reporting other security related issues or concerns to the appropriate lead, or to a member of the **SIRT**.
- Complying with the security policies and procedures of the **Cheshire Federation**. This includes any updated or temporary measures introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent recurrence of an incident).

Security Incident Response Team (SIRT)

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the **Incident Response Lead** of an incident when they receive a security incident report from employees.
- Investigating each reported incident.
- Acting to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analysing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated or adjusted to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

Security Incident Response Checklist

Step 1 – Triage	**Who?**	**Complete?**
1. Determine whether an incident has occurred and the status (suspected, active, contained)		□
2. Prioritise handling the incident based on severity (Refer to **Incident Severity and Category Matrix**)		□
Step 2 – Escalate		
3. Report the incident / convene meeting: i. Critical OR High Severity – escalate to SIRT and also inform [Senior Leadership] ii. Medium severity – escalate to SIRT iii. Low severity – [IT Team] to address as required *External entities may also be required, for example if a criminal act is suspected		□
4. Evaluate risk of data breach for personal or sensitive information related to individuals. Activate the **Data Breach Response Plan** if necessary and not already activated.		□
Step 3 – Respond		
5. Analyse - Learn enough to contain and remediate an attack		□
i. The conditions that lead to the incident		□
ii. The effect of the incident		□
iii. Acquire, preserve, secure, and document evidence		□
6. Contain / Mitigate		□
i. Prevent further effects or spread / lower impact of the issue if possible; OR		□
ii. Determine if further monitoring should be done to collect evidence (case by case)		□
7. Eradicate / Remediate		□
i. Identify and mitigate all vulnerabilities that were exploited. This can include, for example, isolating systems, resetting credentials, blocking traffic, removing malicious files.		□
ii. If more affected hosts are discovered, repeat containment and mitigation steps where required		□
iii. Confirm remediation is successful		□
8. Recover		□
i. Return systems to clean state		□
ii. Confirm affected systems are functioning normally		□
iii. If necessary, implement additional monitoring to check for future related activity		□
Step 4 – Review and Close		
9. Create a follow-up incident report		□
10. Hold a lessons-learned meeting, report and share recommendations with relevant parties		□

Incident Severity and Category Matrix

Incident Severity

Severity	Examples
Critical	- Over 80% of school unable to access technology - Critical systems offline with no known resolution - High risk to / definite breach of sensitive or personal data - Severe reputational damage – likely to impact long term
High	- 50% of staff or students unable to work - Risk of breach of personal or sensitive data - Non-critical systems affected, or critical systems affected with known (quick) resolution - Potential serious reputational damage
Medium	- 20% of staff or students 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 staff or students affected temporarily (short term)

It is important to remember that a security incident is a fluid situation. It may start out **Low** in severity but could escalate to higher levels at a moments notice. You should be mindful of this during the response and mitigation phase. The **IT Manager** and **Incident Response Lead** will be the primary points of contacts in determining the severity on an incident as well as updating its status regularly.

Incident Category

A cyber-attack can take one or several forms. It is important to determine which attack(s) are/have taken place as the type of response is dependent on the attack category. Below is a list of 'typical' attacks carried out.

Category	Examples
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 for the purpose of gathering sensitive information or exposing the network to Malicious Code.
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 business - usually by a sophisticated attacker (often encompassing several of the above categories).
Other	Other incident not listed above

Examples of Incident Response Processes

Some specific incident types require additional response actions – these are listed below. This list should be reviewed regularly with school-specific incident response processes added as necessary depending on the layout of the Network Infrastructure. These steps should be carried out sooner rather than later. The longer a compromised computer is permitted to remain connected to the network, the more damage that can take place and additional incidents become more likely.

Malware (or Malicious Code)

This type of incident may be front-facing e.g. Ransomware where a message will show up on the screen or a malicious program will be visibly running on the computer. Sometimes these disguise as legitimate software but are in fact malicious.

1) Disconnect devices identified with malware from the network immediately. Turn off by holding in the power button for 5 seconds or turn off at the wall. Disconnect the network cable if easy to do so.

2) Identify the malware and examine to identify the type (e.g., rootkit, ransomware, etc.) and establish how it infected the device. This will help you to understand how to remove it from the device.

3) Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device. A whole-network scan is highly recommended to determine if any other endpoints have been compromised.

4) If the malware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by the malware otherwise you will just be re-infecting the infrastructure.

5) Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

Loss of Equipment

1) The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the SIRT and local law enforcement. This includes losses/thefts outside of school hours and at weekends.

2) If the device that is lost or stolen contained sensitive data, and the device is not encrypted, SIRT will complete an analysis of the sensitivity, type and volume of data stolen, including any personal information that has potentially been exposed.

3) Where possible, SIRT will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.) and initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

Denial of Service Attack (DoS)

A denial-of-service (DoS) is any type of attack where the attackers attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends an excessive flood of messages causing servers to come under load, which affects the service being offered.

1) If a DoS attack is suspected, a member of the SIRT must be informed immediately.

2) SIRT will engage with relevant technology leads to review the load and logs of servers, routers, firewalls, applications and other infrastructure as appropriate.

3) SIRT appointed representative to liaise with 3rd party providers as appropriate, if affected.

4) Review technology options available to mitigate the effects of the attack (e.g. temporarily disable bottle neck, increase compute, adjust defences, review filtering options and network DoS prevention features).

5) Once mitigated, document the incident and review to ensure future protection

Non-Compliance with our Security Policy

This covers incidents resulting from deliberate or accidental actions that are in breach of our security policy and which put sensitive data at risk. This includes any systems or data misuse, unauthorised exposure of data to external parties, unauthorised changes to systems or data.

1) SIRT will engage with the relevant business area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.

2) SIRT and/or line managers will notify People and Engagement of the incident.

3) SIRT will liaise with People and Engagement and line managers to determine whether disciplinary action is needed.

4) SIRT will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example re-training of employees.

Sustained attack by using multiple vectors

If under sustained attack through multiple vectors (e.g. malicious code is used to then gain access to data which is then encrypted):

1) SIRT to convene and review all symptoms of attack

2) Incident Response Technical Lead to assign technical resources as necessary in order to mitigate and recover from attack

3) Technical resources to report to Incident Response Technical Lead and collaborate to mitigate against further incidents

4) Incident Response Technical Lead and Technical Resources to collaborate on root cause analysis and report back to SIRT

5) SIRT will undertake an assessment of the impact and conduct a risk analysis against remaining or newly discovered vulnerabilities and implement controls as necessary

Unauthorised Wireless Access Points

If unauthorised wireless access points are detected, or reported by employees, these must be recorded as a security incident.

1) SIRT will investigate to identify the location of the unauthorised wireless access point/device.

2) The SIRT will investigate as to whether the unauthorised wireless access point/device is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the business justification is documented and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).

3) All other unauthorised wireless access points/devices must be located, shutdown and removed.

Resources for Staff Training

37 Minute video for Cyber security training for school staff -
https://www.youtube.com/watch?v=pP2VKWSagE0

PowerPoint version of the video above
https://www.ncsc.gov.uk/files/cyber-security-training-for-school-staff.pptx

Additional Resources
https://www.ncsc.gov.uk/information/resources-for-schools

Cybersecurity Incident Notification Form

Name:

Date of incident:

Time of incident:
(As accurate as possible)

Date of reporting (Today):

Username logged on:

Was personal data involved in the incident?

Nature of the incident:
(Tick all that apply)

E-Mail based	
Phone based (Excludes Teams/Zoom)	
Website based	
Software based	
Hardware based (USB/Laptop etc)	
Unsure/Other	

Has the device been isolated?
(Turned off and removed from general use)

Brief description of what happened and what actions you took if any:

Location incident occurred:
(Home/School/Other)

Device affected:
(PC/Laptop/Tablet/Other)

Device location:

Asset Number:

Signed:

Date:

Time: