**Contents**

[**1.** **Understanding Events and Incidents** 3](#_Toc165461535)

[**2.** **Detection** 3](#_Toc165461536)

[**3.** **Reporting Requirements** 3](#_Toc165461537)

[**4.** **Reportable Incidents** 4](#_Toc165461538)

[**5.** **External Reporting** 5](#_Toc165461539)

# **Understanding Events and Incidents**

Not all events are incidents. An **event** is anything which is observed on your network - updating your anti-virus is an event. An event *may*lead to a potential incident and an incident might be a series of events with an *adverse* effect.

It is essential to detect events and make sense of them. This allows you to determine what the appropriate response should be and make decisions on whether any adverse effect is likely. Events might seem minor, but logging them evidences any trends which can prompt policy or security changes and inform user training.

An **incident** could be a virus attack, malware, ransomware, hacking, unauthorised access to systems, environmental disaster, DDoS attack, or theft.

Staff should ensure they are confident with reporting mechanisms and there should be an understanding of risks.

# **Detection**

Threat detection is vital to reducing the likely impact of any incident. The following steps all support threat and vulnerability detection:

* Run anti-virus checks and malware checks regularly and review any notifications.
* Strong firewall rules and intrusion detection systems, such as the Police Cyber Alarm\* will provide early alerts.
* Ensure staff have cyber-awareness training and know how to manage and report alerts.
* Log files can help you detect multiple failed logon attempts, show applications and device errors, and detect changes in use.
* Look for changes in email use or an increase in spam.
* Check your filtering / proxy server logs to look for inappropriate searches, or users continually attempting to access inappropriate content.
* Communicate with other schools to keep alert to current threats.

# **Reporting Requirements**

In order to respond appropriately to incidents, Senior Leaders must be made aware of any issues or potential threats. This allows prompt investigation and effective incident management:

1. Reporting processes should be clearly defined
2. Templates for reporting should be readily available
3. All users should be aware of their reporting obligations and understand how, when, and to whom they should report.

Internal monitoring of alerts for events and potential incidents should feed into the incident reporting process.

Ensure IT Support Technicians / external IT staff understand their responsibility to report to senior leaders. It is vital that senior leaders have whole over-sight of their networks and any potential security threats. This helps to inform expenditure and support a proactive response.

# **Reportable Incidents**

The following is a list of the types of incidents which should be reported:

**Suspicious events** These may include unusual memory usage, notifications, or pop-ups.

**Suspicious emails** May prompt receivers to click links or download unexpected attachments. Often have poorly written English, appear similar to recognised email addresses, and often request confirmation of security credentials or other sensitive information.

**Unauthorised access** Deliberate / criminal attempts, such as hacking or via unauthorised sharing of credentials.

**Security breaches** Attempts to circumvent school security (includes staff / pupils).

**Illegal activity** Downloading or installing unlicensed software / applications. Accessing illegal content or inappropriate sharing.

**Vandalism** Any deliberate acts which affect hardware or computer systems. This may include the malicious deletion of files.

**Hardware damage** Damage to hardware due to any cause. This may be accidental, due to vandalism, tampering, or from disaster such as flooding.

**Defamatory/abusive** Communications via email, chat functions or other digital platforms

**Communications** which are derogatory, persistent and/or abusive.

**Virus / malware alerts** Users seeing alerts from anti-virus or anti-malware should report these and ensure actions are being taken to resolve the issue.

Reporting and escalation processed should be clearly documented and well communicated.

# **External Reporting**

If you have been the victim of a ransomware or other cyber incident, please take the following steps immediately:

1.   Enact your incident management plan

a.   Contact your insurance provider if you have cover.

b.   If you are a part of a Local Authority (LA) please contact your LA.

2.   Contact your local law enforcement and Action Fraud, via <https://www.actionfraud.police.uk/>

3.   Contact a Cyber Incident Response (CIR) company as soon as possible. Some CIR companies certified by the NCSC can be found [here](https://www.ncsc.gov.uk/section/products-services/all-products-services-categories?productType=Cyber+Incident+Response+%28CIR%29).

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

**If there is a suspected personal data breach then please inform the ICO either online via** [**www.ico.org.uk**](http://www.ico.org.uk/) **or contact them via their helpline on 0303 123 1113 within 72 hours.**