**IT Incident Management Guide**

V2.0

**Contents**

[**1.1** **Introduction** 3](#_Toc77685409)

[**1.2** **Aims** 3](#_Toc77685410)

[**1.3** **Objectives** 3](#_Toc77685411)

[**1.4** **Events and Incidents** 3](#_Toc77685412)

[**1.5** **Detection** 4](#_Toc77685413)

[**1.6** **Reporting and Recording** 4](#_Toc77685414)

[**1.6.1** **Information to include in an incident log** 5](#_Toc77685415)

[**1.7** **Analysis** 6](#_Toc77685416)

[**1.7.1** **Impact and Severity Categorisation** 6](#_Toc77685417)

[**1.7.2** **Severity Classifications** 7](#_Toc77685418)

[**1.7.3** **Impact Assessment** 8](#_Toc77685419)

[**1.8** **Handling the Incident** 9](#_Toc77685420)

[**1.8.1** **Actions to contain and remove threats** 9](#_Toc77685421)

[**1.8.2** **Recovery** 9](#_Toc77685422)

[**1.9** **Lessons Learned - Post Incident Review** 10](#_Toc77685423)

# **1.1 Introduction**

As cyber-attacks and incidents increase in the education sector, there is a need to provide staff with a method for responding to incidents in a prompt and organised manner. An effective response minimises pressures on staff and systems, mitigates the effects of any incident, and facilitates a return to the normal methods of working promptly and efficiently.

Schools should plan to contain, handle, and respond to incidents prior to this being a necessity. Communicating any plans with staff, and training staff to understand their role in any plan is vital.

# **1.2 Aims**

To manage and respond to unexpected and disruptive events in order to minimise the impact and maintain school functions at an acceptable level.

# **1.3 Objectives**

* Prepare for an IT incident
* Detect and identify incidents appropriately
* Recording and reporting events and incidents
* Investigating and managing incidents
* Reacting and handling the incident
* Recovery
* Lessons Learned

No school will ever be able to remove the possibility of an IT Incident. It is inevitable that incidents will occur, and some may be serious. Effective identification, classification, and planning is essential to maintaining school functions and protect the reputation of the school.

Incidents can be:

* Cyber-attacks, such as viruses, denial of service (DoS), or ransomware
* The result of human error, accidents / disasters, or system failure

While it is important for organisations to have preventive measures in place to avoid security incidents, it is equally important that there is a robust and practised response plan should an incident occur.

This document should be read in conjunction with the school’s Disaster Recovery Plan

# **1.4 Events and Incidents**

An information security event is anything which could lead to a potential incident. An incident might be a series of events with an adverse effect.

It is essential to detect events and make sense of them to determine what the appropriate response should be. Events might seem minor but logging them evidences any trends which can prompt policy or security changes and inform training.

An event could be a system crash, unauthorised access to systems / data or a breach of policy.

An information security incident could be a virus attack, malware, ransomware, hacking, environmental disaster, DDoS attack, or theft.

Events and incidents are most often caused by human error. Staff should ensure they are confident with reporting mechanisms and understanding risks.

# **1.5 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. \**Cyber Alarm can be arranged without charge via S4S*
* 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
* Communication with other schools to keep alert to current threats

# **1.6 Reporting and Recording**

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:

* Reporting processes should be clearly defined
* Templates for reporting should be readily available
* 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 oversight of their networks and any potential security threats. This helps to inform expenditure and support a proactive response.

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 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** | Communications via email, chat functions, or other digital platforms. |

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

An example reporting form is included as part of this guide.

## **1.6.1 Information to include in an incident log**

1. Date and time when the incident occurred (if known)
2. Date and time when the incident was discovered/detected
3. Date and time when the incident was reported

*(Remember that logs may record times in different time zones)*

1. The physical location of the incident or system
2. Is there a risk to data and information?
3. Has any sensitive data been accessed, lost, or changed?\*
4. Is the incident time bound or on-going?
5. Scope, impact, and severity assessment
6. Source or cause of the incident (if known)
7. Description of the incident (e.g. how it was detected, what occurred)
8. List of files / systems / networks / applications affected
9. Summary of actions taken
10. Date and time the incident was resolved

\* GDPR / DPA 2018 requires schools to take the necessary technical and organisational measures to ensure a high level of information security. Personal data breaches may need to be reported to the ICO within 72 hours.

# **1.7 Analysis**

The analysis should gather all relevant information to confirm the details of the incident.

Record the verified facts and avoid speculation. Be aware that in some cases, documents may be required for legal proceedings.

Sometimes initial analysis leads to a more comprehensive investigations and possible escalation or further actions. Investigative steps may continue after systems have been restored. Investigations will vary in length and complexity and may involve external agencies, such as the police, social care, or safeguarding teams.

Depending on the type of incident, third parties may also be affected and may be able to supply information. Consider the benefit of additional information and any potential implications from third party involvement.

The educational professional’s helpline can offer support on: 0344 381 4772 or message: helpline@saferinternet.org.uk.

## **1.7.1 Impact and Severity Categorisation**

Determining the scope of the incident is about assessing the damage and impact of the incident in order to limit any further damage and mitigate any effects.

A severity categorisation considers the impact on school functions / services such as:

* How many users are affected?
* How many systems are affected and how critical are they?
* Are there are potential safeguarding implications?
* Can the school remain open?
* Is there any likely reputational impact?
* What is the financial impact, considering the repair cost and equipment replacement?

The severity level should be defined so senior leaders understand when an incident should be escalated. If the incident has led to a significant impact to facilities and / or services, which can’t be recovered in standard timescales, schools should refer to and enact their Disaster Recovery Plan.

## **1.7.2 Severity Classifications**

**Critical** **An incident which is vital to the functioning of the school**

Affects large numbers of users (80%+)

Involves a serious security breach

Actual or high risk of personal data breach

Affects critical IT systems

Noticeable financial loss

Likely to lead to reputational damage

**High An incident which involves half of users**

 Risk of personal data breach

Disrupts services which are not vital to the functioning of the school but impacts significantly

Likely financial implications

Potentially lead to reputational damage

**Medium An incident that involves some uses or parts of the school**

 Risk of a data breach which may involve personal data

 Disruption to non-essential services / facilities

 Possible short-term reputational impact

 Resolution is possible within the shorter term

**Low An incident that can be routinely contained, handled, and resolved.**

 Low numbers of users / device affected with minimal disruption

**It is important to log all classifications of events / incidents regardless of severity**

## **1.7.3 Impact Assessment**

|  |  |  |
| --- | --- | --- |
| **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. |

# **1.8 Handling the Incident**

It is essential to contain incidents, this means taking immediate steps to reduce the impact of any incident.

The school will need to tailor their actions depending on the type of incident and the risks posed. Bringing all affected systems back to full functionality requires a logged, step by step approach.

## **1.8.1 Actions to contain and remove threats**

* Changing system administration passwords where admin accounts are compromised
* Removing any accounts / backdoors left by any attackers
* Blocking and logging any unauthorised access
* Blocking malware sources which may include email addresses and infected websites
* Closing ports
* Stopping traffic flow from infected mail servers
* Checking proxy server settings / firewall filtering
* Redirecting website homepages if the school website has been hijacked
* Isolating systems and disconnecting infected devices from the network
* Allowing sufficient time to ensure that there is no response from the attacker
* Identify all affected systems beyond the organisation so that third parties are informed

If a server is affected the school may be able to route traffic to failover servers. If this is not possible, the impact on school functions will be more extensive and the severity classification will be higher.

It may be necessary to disconnect affected systems by removing the network cable or powering down switches and/or routers. Shutting down the power to a computer should only happen with guidance from IT technicians / support staff, as evidential data may be lost.

It is also essential that the cause of the incident has been addressed, where possible, and any required changes have been implemented to address vulnerabilities.

## **1.8.2 Recovery**

1. Resetting passwords on compromised accounts
2. Rebuilding / repairing infected systems
3. Replacing compromised files with clean, uninfected files from tested backups
4. Removing any temporary constraints imposed on systems, access, and users
5. Installing patches, security updates, network security, firewall rules
6. Testing systems thoroughly to confirm systems are clean and fully functioning
7. Follow-up any statutory reporting / regulatory actions
8. Review and monitor

# **1.9 Lessons Learned - Post Incident Review**

Consider whether the incident could have been avoided. The follow-up to any incident should be to look at:

* Staff awareness of the procedures
* Procedure implementation by staff
* Assessment of which security controls failed
* Efficiency of reporting mechanisms
* Effectiveness of the response
* Statutory reporting
* Policy and procedure review
* Risk assessment review
* Evaluate effectiveness of communication throughout the incident
* Time taken for recovery
* Staff awareness and training