

# TIBSHELF COMMUNITY SCHOOL CYBER SECURITY

Ratified: July 23  
(DCC Policy)



## 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.

Tibshelf School 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.

## Aims

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

### 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 protecting 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, practised response plan should an incident occur. This document should be read in conjunction with the school's IT Disaster Recovery Plan and the Critical Incident Plan.

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

## Mitigation

The school will take steps to prevent systems becoming compromised. These will include but are not limited to.

- Boundary firewalls and internet gateways — Network perimeter defences, particularly web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet.

- Malware protection — Malware defences to detect and respond to known attack code.
- Patch management — patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software bugs.
- Whitelisting and execution control — prevent unknown software from being able to run or install itself, including AutoRun on USB and CD drives.
- Secure configuration — restrict the functionality of every device, operating system and application to the minimum needed for business to function.
- Password policy — ensure that an appropriate password policy is in place and followed.
- User access control — include limiting normal users' execution permissions and enforcing the principle of least privilege.

## 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 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 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 and Recording

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:

<b>Suspicious events</b>	These may include unusual memory usage, notifications, or pop-ups
<b>Suspicious emails</b>	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.
<b>Unauthorised access</b>	Deliberate / criminal attempts, such as hacking or via unauthorised sharing of credentials.
<b>Security breaches</b>	Attempts to circumvent school security (includes staff / pupils).
<b>Illegal activity</b>	Downloading or installing unlicensed software/applications. Accessing illegal content or inappropriate sharing.
<b>Vandalism</b>	Any deliberate acts which affect hardware or computer systems. This may include the malicious deletion of files.

<b>Hardware damage</b>	Damage to hardware due to any cause. This may be accidental, due to vandalism, tampering or from disaster such as flooding.
<b>Defamatory/abusive communications</b>	Communications via email, chat functions or other digital platforms

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.
4. *(Remember that logs may record times in different time zones)*
5. The physical location of the incident or system
6. Is there a risk to data and information?
7. Has any sensitive data been accessed, lost, or changed? \*
8. Is the incident time bound or on-going?
9. Scope, impact, and severity assessment
10. Source or cause of the incident (if known)
11. Description of the incident (e.g., how it was detected, what occurred)
12. List of files / systems / networks / applications affected.
13. Summary of actions taken
14. 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.

## 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, 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@saferrinternet.org.uk](mailto:helpline@saferrinternet.org.uk)

## 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 take 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.

## Severity Classifications

<u>Critical</u>	<p>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.</p>
<u>High</u>	<p>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 impact significantly.          Likely financial implications          Potentially lead to reputational damage</p>
<u>Medium</u>	<p>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.</p>
<u>Low</u>	<p>An incident that can be routinely contained, handled, and resolved.          Low numbers of users / device affected with minimal disruption.</p>

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

## Impact Assessment

<b>Operational</b>	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 <b>some</b> 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.
<b>Informational</b>	No Breach	No information has been accessed / compromised or lost.

	Data Breach	Access or loss of data which is <b>not</b> 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)

<b>Restoration</b>	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.

## 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.

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.

### **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.

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

Consider whether or not 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
- 

## Appendix 1

A.1 Computer Misuse Report Form

Reference:

**All details will be treated as strictly confidential.**

**\* Denotes a mandatory field. This must be completed in order to submit the report.**

Are you reporting misuse of school or setting IT facilities/services, or misuse of an external institution's facilities/services? \*

What type of misuse are you reporting? \*

- Attempt to gain unauthorised access to facilities/services.
- Abusive activity/material
- Defamatory or libelous activity
- Illegal activity (inc illegal downloads / installations)
- Tampering with software / hardware
- Vandalism
- Other activity


Date of the misuse:

Time of the misuse:

Location of the misuse: *This may include rooms / offices / on-site, off-site.*

**Please provide details of the misuse, giving as much detail as possible.**





**Have you reported this to anyone else? If so, please state when and to whom:**

Please enter your contact details below.

Your name

Your organisation (if reporting from outside the school)

Your email address

Your telephone numbers.

In line with the GDPR and Data Protection Act 2018, the details submitted on this form will only be used for investigating the reported computer misuse and for statistical purposes.



**Appendix 2**

A.2 IT Security Incident / Concern Form

Reference:

**Names of all relevant staff / pupils concerned.**

**Date of Incident or Concern:**

**Time:**

**Reported by:**

**Role:**

**Is this incident a:**

- **Safeguarding Concern**
- **Filtering Issue / Unsuitable Content**
- **Security Threat / Cyber-attack**
- **Virus / Malware Report**

- 

**Other**

**Location of Incident / Concern:**

**Description of Incident / Concern:** (incl. equipment, what was said and by whom)

**Other Information:** (previous history / log references / background information)

IT Provider / Technician Informed?

Name of contact and date:

Action taken and by whom:

(For more significant incidents please complete the disaster recovery actions log)

LA referrals, if applicable (name dept):

Third party referrals / agencies - Please specify ALL referrals and the date.

Referral 1

Referral 2

Referral 3

Date:  
Outcome referral 1

Date:  
Outcome referral 2

Date:  
Outcome referral 3

Signed / Initialled by investigator:

Signed / Initialled by SMT:

Log Completed      Date: \_\_\_\_\_      Actions Completed      Date: \_\_\_\_\_

Additional notes / suggested changes to policy / procedure

Please ensure copies of all related correspondence and third-party referrals are filed with this report.

Headteacher	01773 872391
Designated Safeguarding Lead	01773 872391
Co-Chair Governors	01773 872391
Site Manager	01773 872391
Caretakers	01773 872391
Network Manager	01773 872391
Senior ICT Technician	01773 872391
Information Manager	01773 872391
Business Manager	01773 872391
DCC IT Helpdesk	01629 537777 or 01629536789 Services.desk@derbyshire.gov.uk
Action Fraud (Reporting Cyber Crime)	030012320740 <a href="http://www.actionfraud.police.uk/">www.actionfraud.police.uk/</a>
Safeguarding for School advisor DSCB Protection Manager for Schools	
Cyber Protection Officer	
Local Authority Designated Officer (LADO)	
IT Provisions / Supplier	Stone Computers Ltd 0844 822 1122