connecteducationtrust.org

Cybersecurity Incident Response Plan Guidance

Academic Year 2022-2025

Purpose

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity guidelines and security provisions which are there to protect our systems, services, and data in the event of a cyberattack.

Scope of policy

This guideline applies to all staff, contractors, volunteers, and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Connect Education Trust also implements practices designed to proactively reduce the risk of unauthorised access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection and numerous other industry standard systems.

In the event of a cyber security incident, staff have been trained to expeditiously deal with the matter. Staff are trained on a yearly basis to report any such possible Incident to Senior Leaders so the Incident Response can be mobilised. Throughout the year the leaders are kept up to date on the latest security threats and trained in modern techniques of incident remediation.

The availability and protection of the information resources managed by the systems we maintain is of paramount importance to our Trust and will always be a core value of our organisation.

Risk Management

Cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to the Board of Trustees.

Physical Security

The Trust and its schools will ensure there are appropriate physical security and environmental controls protecting access to its IT Systems, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, the Trust and its schools will maintain asset registers for files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform IT Support/ SLT as soon as possible. Personal accounts should not be used for work purposes. Schools will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to (IT Support)
- Change all account passwords at once when a device is lost or stolen (and report immediately to (IT Support)
- Report a suspected threat or security weakness in the systems
- Devices will be configured with the following security controls as a minimum:
    - Password protection
    - Full disk encryption
    - Client firewalls
    - Anti-virus / malware software [e.g. Sophos and Malwarebytes for LGfL schools – see sophos.lgfl.net / malwarebytes.lgfl.net]
    - Automatic security updates
    - Removal of unrequired and unsupported software
    - Autorun disabled
    - Minimal administrative accounts

Sharing flies

Recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping files on school systems
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting IT Support/DPO to any breaches, malicious activity, or suspected scams

Training

Recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams. (LGFL offer Cyber Security Training for School Staff and Sophos Phish, a phishing simulation tool that links to training material).

School Role

- Regularly reviews Online Safety Guidance and Data Protection Policy.
- Assess the school's current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role-based user access.
- Implement a regular patching regime: Routinely install security and system to ensure any internet-facing device is not susceptible to an exploit. This includes exchange servers, web servers, SQL servers, VPN devices and
- Firewall devices - Ensure that security patches are checked for and applied on a regular basis.

- Staff to recognise, report, and appropriately respond to security messages and/or suspicious activities
- Staff training updated yearly

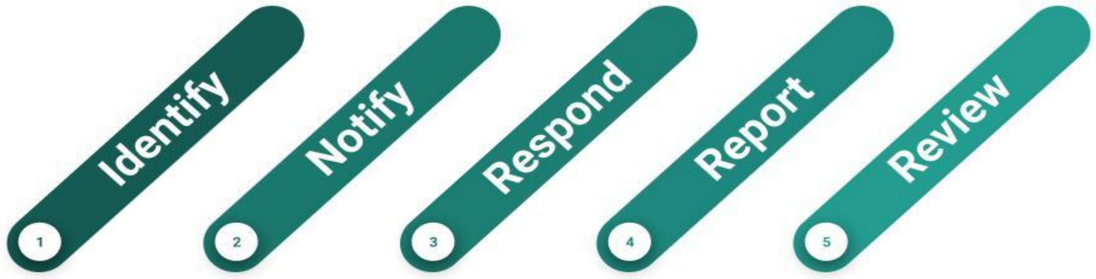
Cyber Security Incident

A Cyber Security Incident is any event that threatens the confidentiality, integrity or availability of the information resources we support or utilise internally, especially sensitive information whose theft or loss may be harmful to individual students, our partners or our organisation.

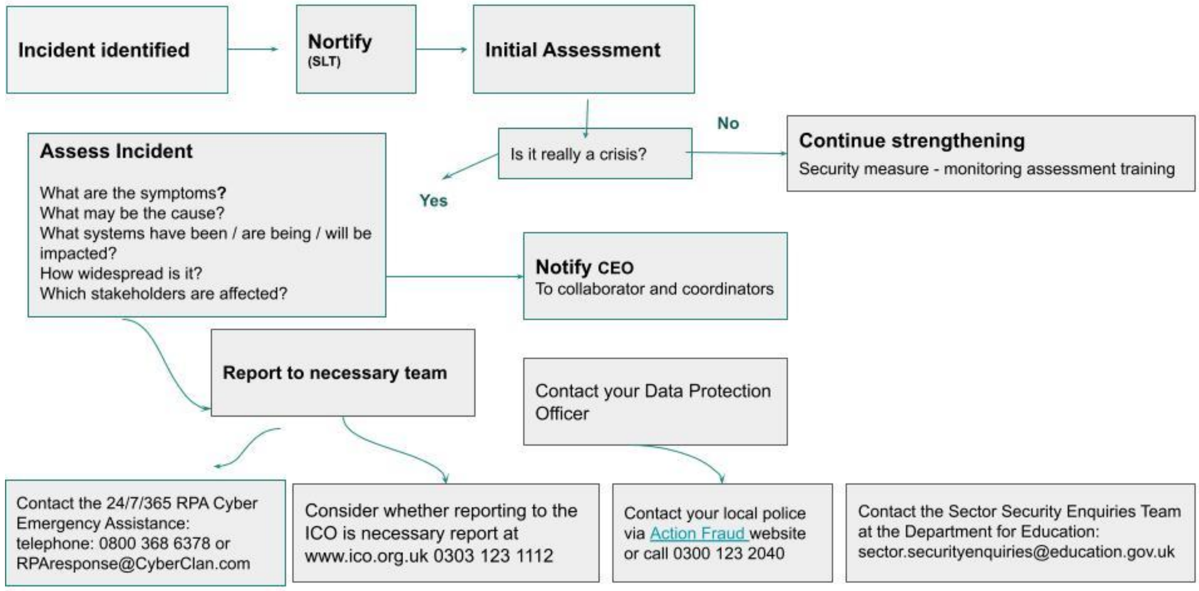
Common Types of Security Incident

Incident type	**Description**
Malware	Malicious software (viruses, worms, trojans, etc.) that gets unauthorised access to your systems and disrupts operations.
Distributed denial of service (DDoS)	Makes your online service (e.g., website) unavailable by overwhelming your server with more traffic than it can handle.
Phishing	A social engineering attack that dupes users to believe malicious emails as legitimate.
Web application attack	Attacks your web applications such as shopping carts, online forms, and word processors to gain access to your databases and steal sensitive information.
Insider threat	Current or former employees violating IT security policies to gain unauthorised access, leak confidential data, or damage systems.
Loss or theft of equipment	Lost or stolen devices that can be misused to seal data or launch full fledge cybersecurity attack

Actions in the event of an incident



Actions in the event of an incident



Incident identified

Nortify (SLT)

Initial Assessment

Is it really a crisis?

No

Continue strengthening
Security measure - monitoring assessment training

Yes

Assess Incident

What are the symptoms**?**
What may be the cause?
What systems have been / are being / will be impacted?
How widespread is it?
Which stakeholders are affected?

Notify CEO
To collaborator and coordinators

Report to necessary team

Contact your Data Protection Officer

Contact the 24/7/365 RPA Cyber Emergency Assistance:
telephone: 0800 368 6378 or RPAresponse@CyberClan.com

Consider whether reporting to the ICO is necessary report at www.ico.org.uk 0303 123 1112

Contact your local police via Action Fraud website or call 0300 123 2040

Contact the Sector Security Enquiries Team at the Department for Education:
sector.securityenquiries@education.gov.uk

Action Plan

Action	Timing	Responsible	Complete
Verbal notification of incident/ or identifies a problem through system alerts	Immediate		
Notify Key services or stakeholders	Immediate		
Respond/ Assessment of scope of incident and options for limiting impact	Within 1 Hour		
Review recovery priorities	Within 1 Hour		
Communicate with school staff Inform Action Fraud	Within 1 Hour		
Estimated recovery time/ invoke full or partial recovery plan	Within 1 Hour		
Communicate with parents if required as part of school day	Within 2 Hours		
Regular updates	🟧		
Communicate with Public bodies as required	🟧		

Identify

Incident Types of cyber incidents that may threaten the organisation are:

- Unauthorised attempts to gain access to a computer, system, or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorised access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, corruption, or unauthorised distribution

Incident Symptoms Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness • Unexplained lockouts, content, or activity
- Locally hosted websites won't open or display inappropriate content or unauthorised changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behaviour or activity by XXXXXXX staff, students, partners, or other actors

Notify - Assess

Considerations

- What are the symptoms?
- What may be the cause?
- What systems have been/ are being/ will be impacted?
- How widespread is it?
- Which stakeholders are affected?

Documentation

Regardless of whether it is determined there is a security threat, SLT will accurately document the scenario in a Cyber Security Incident Log. All Cyber Security Incident Logs will be stored so incident information may be reviewed in the future. This report should contain information such as:

- Who reported the incident?
- Characteristics of the activity
- Date and time the potential incident were detected
- Nature of the incident
- Potential scope of impact
- Whether the SLT is required to perform incident remediation?

Respond

Upon determining that a significant incident or breach has occurred, the Headteacher or SLT member should be notified immediately. As additional information is uncovered throughout the investigation, staff should be briefed by the SLT so appropriate decisions are made.

Initial Response

These first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve measures up to and including immediately disconnecting workstations, servers or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas to define the entire scope of the incident.

Report

The Incident Summary Report will include all information to the incident, but at minimum:

- Dates and times of milestones throughout the process (e.g., incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

Review

Post-Incident Review Meeting

After the conclusion of the incident and discuss the event in detail, review response procedures and construct a Process Improvement Plan to prevent a recurrence of that or similar incidents. The compiled Incident Report constructed by the Headteacher will serve as a guide for this meeting. In the meeting, a full debrief of the incident will be presented and findings discussed. The Headteacher will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan. The group will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

Process Improvement Plan

The Headteacher will draft a Process Improvement Plan based on the results of this meeting. The plan should discuss any applicable items necessary to prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The Process Improvement Plan will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately. Areas of focus may include, but are not limited to:

- New hardware or software required
- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan

Recovery Priorities

This section details the order in which systems should be restored to ensure that critical functions are available as soon as possible. As different systems have different priorities.

Sample

System/Service	Pre-requisites	Priority	Notes
Backup solution		Very High	
Active Directory/User account administration	Backup solution	Very High	Required for the majority of other services
Google Workspace Email/OneDrive/G Drive	Active Directory (depending on configuration)	Very High	
Management Information System	Active Directory	High	
Phone system		High	Not integrated to other systems
User files	Active Directory	Medium	
Access control			Not integrated to other systems
CCTV		Medium	Not integrated to other systems
Education Apps	Active Directory	Low	
Printing	Active Directory	Low	
Cashless catering			
Safeguarding			
SEND			

Key Services Providers (School to update)

This section provides a record of key service providers that form part of the school's IT services.

This table should be updated to include details of all your school's service providers who may need to be involved in the response to a major incident.

Name	Type /description of service	Contact details	Notes
Police – Action Fraud	National reporting centre for fraud and cybercrime	0300 123 2040	Available 24/7 for businesses
LA/Borough/Trust			
Information Commissioner's Office	Regulatory office in charge of upholding information rights.	ICO breach reporting website 0303 123 1113	Will need to be informed within 72 hours if data has been stolen during the incident.
LGFL	Internet connectivity and security product licensing	020 82 555 555 Option 5 Support site	
BT	Phone lines		
Sophos	Antivirus solution	Sophos Central	
Malwarebytes	Antimalware solution	Malwarebytes	
Grid store	Cloud backup solution		
Hardware reseller			
Third party support organisation			
Licensing provider			
CCTV provider			
Access control provider			

TEMPLATE

Incident Summary Report

Categories	Information
Type of Incident	
Date Incident Was Detected	
By Whom Was Incident Detected	
How Was Incident Detected	
Scope of Incident (Districts / Systems Affected)	
Date Incident Corrected	
Corrective Action Types (Training, Technical, etc)	

Summary of Incident Symptoms

Summary of Incident Type and Scope

Summary of Corrective Actions

Process Improvement Plan

Areas of Success Summary

Areas in Need of Improvement Summary

Recommended Improvements to Avoid Future Incidents

Recommended Improvements to the Cyber Security Incident Response Plan

Action Incident Log

Date	Time	Description of the event/action taken/decision made	Costs incurred	Completed by

Sample Parent Letter

Dear Parents,

This letter is to inform you of an incident that occurred within the XXXXXXX. This incident resulted in student/staff/etc data being compromised by an outside entity. Our team acted quickly to assess and mitigate the situation. Currently, we are able to share the following details:

[insert a brief description of the breach or unauthorised release, the dates of the incident and the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate]

Please know that XXXXXXX is committed to protecting and securing educational data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your child's educational records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident from occurring in the future.

Please contact XXXXXXX with any questions you may have regarding this incident and our response.

Kind regards,