Cyber Security Incident Management Plan

Learning4Life-Gy

Version 2.3 – 2022 Copyright Secure Schools Ltd.

Contents

Learning4Life-Gy

1.0. Introduction

Information Technology is crucial in supporting the smooth running of administrative and business operations within a Learning4Life-Gy. Successful cyber-attacks targeting a school's information assets threaten to severely disrupt normal operations. Responding effectively to a cyber security incident requires a coordinated effort, engagement, additional resources, and technical expertise. This document provides clear guidance and procedures that Learning4Life-Gy will follow in response to a cyber security incident.

2.0 Aim

This cyber security incident management plan aims to:

- Prompt regular discussions about critical data and systems
- Give Learning4Life-Gy the best chance of resisting disruption to students' education
- Define what Learning4Life-Gy considers a cyber security incident
- Assess risk and minimise the impact of the incident
- Ensure a systematic, swift, and effective response
- Restore normalcy as quickly as possible
- Coordinate response activities, document findings, and to notify appropriate stakeholders

3.0 Defining a Cyber Security Incident

Learning4Life-Gy considers three requirements when designing and implementing security measures: *confidentiality*, *integrity*, and *availability*. Violation of one of these principles compromises the security of a computer system and is considered a cyber security incident.

Security Requirement	Violation Example
Confidentiality	Evidence of a data breach resulting in sensitive or protected information being stolen, copied, or transmitted by an unauthorised person.
Integrity	Evidence of unauthorised alterations to the school's data.
Availability	Outage of some or all the school's systems, and therefore not accessible for regular teaching or administrative functions.

4.0 Impact Assessment

	Level	Violation example	Response type
Critical	Very High	• Severe breach of the Learning4life-gy's information security policy or objectives, usually resulting in the exposure of personal information or any form of sensitive data. • severe disruption of normal school operations (e.g., staff unable to teach) • severe financial or reputational damage	• Immediate response from all the members of the incident management team • External incident response team involvement • Involvement of relevant authorities • Probable insurance claim
	High	• Significant breach of the Learning4life-gy's information security policy or security objectives, with the potential exposure of confidential data • financial or reputational damage • disruption of normal school operations (generally resolved within a reasonably short time)	• Immediate response from all the members the incident management team • Possible external incident response team involvement • Probable involvement of relevant authorities • Possible insurance claim
Non-critical	Medium	• Breach of the Learning4life-gy's information security policy or security objectives, with the potential exposure of internal data • Low financial or reputational damage • Minimal disruption and possible breach of non-sensitive data	• Might include all or some members of the incident management team • External parties may be involved • Possible involvement of relevant authorities • Possible insurance claim
	Low	• Minor breach of the Learning4life-gy's information security policy or objectives with no evidence of damage caused • No financial or reputational damage • Non-critical systems affected	• Usually handled by the IT team but might include incident response team members • Authorities not involved • No insurance claim

5.0 Planning and Preparation

A well-planned and coordinated response is key to effectively reducing the impact of a cyber security incident. Planning and preparation should also focus on preventing the incident in the first place. Learning4Life-Gy reviews this plan annually, or in the event of a major system or personnel change.

5.1 Prevention

Learning4Life-gy implements the following, which have been extracted from its Cyber Security Policy:

- At least annual reviews of Information Security and Data Protection Policies. Where appropriate, the Learning4life-gy consults a subject matter expert.
- Cyber security policies, procedures, and practices are aligned to recognised standards such as Cyber Essentials or IASME Cyber Assurance.
- Where supported, as an additional layer of security, the Learning4life-gy enables and enforces multi-factor authentication for all online accounts.
- Learning4Life-gy maintains a patch management policy that aims to install all critical and high severity updates within 14 days of release. Where possible, auto-updates for operating systems and applications are enabled. This applies to all laptops, desktops, servers, mobile devices, and firewalls.
- Learning4Life-gy monitors all services accessible externally through the firewall. All systems that process potentially sensitive information should have a business case before being allowed through the firewall and be reviewed regularly. External RDP access is discouraged, but where this is allowed, this is secured by:
    - Implementing multi-factor authentication
    - Restricting access only to specific public IP addresses
    - Configuring a lockout mechanism after ten or more unsuccessful login attempts.

5.2 Documentation

Network architecture

Learning4Life-gy maintains up-to-date documents detailing the network architecture with network diagrams that provide helpful information during a cyber incident. The Learning4life-gy's network architecture documents detail all IP ranges, VLANs, location, internet gateways, critical systems, and servers.

This is especially important because it enables a faster response and easier communication for handover to any outside supporting party or incident response team.

Asset register

Learning4Life-Gy maintains an up-to-date information asset register that details the location, owner, and security requirements. This register will be helpful when trying to understand the affected assets.

5.3 Logging

Log data is computer-generated data about essential activities and patterns within operating systems and software applications that can be used to analyse trends, access activity, and predict future events. Learning4Life-gy aims to review essential logs at least weekly. In the case of a cyber security incident, logs provide a good picture of how a breach occurred.

5.4 Backup, Contingency and Recovery

Backup systems are a vital part of data recovery, and Learning4Life-Gy aims to implement the following in line with the NCSC backup guidance:

- Having offline backups, preferably offsite
- Keeping a record of the data that the Learning4life-gy backs up and ensuring that critical data is part of the backup
- Having multiple copies of the same file using different backup systems
- Regularly testing backups to ensure they align with the business continuity plan.

Information Asset	Why is this Critical?	Backup Type	Backup On-site/ Off-site	Backup Frequency	Recovery Point & Time Objectives	Contingency
File Server(s)	*The file servers provide access to lesson plans and teaching resources that, if unavailable, would cause significant disruption.*	*Remote*	*off-site*	*Daily*	*1 hour to access all data required.* *24 hours to full backup restore*	*Data streaming from online remote backup solution*

5.5 Insurance Cover

Learning4Life-gy recognises that the effectiveness of its response to an incident is reliant on the availability of resources around the time of the incident. The Learning4life-gy has decided not to acquire an insurance policy for cyber security related incidents.

5.6 Legal and Regulatory Requirements

Cyber security incidents often require different responses based on the type of incident and the impact. Learning4Life-gy is bound by the UK's data protection regulation requirements and legislation such as the GDPR and DPA, therefore part of the planning includes having a clear understanding of the data the Learning4life-gy holds and if the data is appropriately secured. Planning under this area also includes:

- Understanding the type of incident(s) that needs to be reported to avoid further consequences *e.g., reporting to the ICO within 72 hours of being aware of an incident that has a potential risk to people's rights and freedoms.*
- When and how to seek legal support.
- How to isolate data to preserve it for forensic examination (aligned with ACPO Guidance for handling digital evidence).

5.7 Assembly Point

It is essential to designate a meeting point where the incident response team will operate from. The chosen location should have the facilities and resources the incident management team might need. In the case that the team cannot meet at a particular physical location, alternative tools must be selected which allow the team to meet virtually but securely and with minimum disruption.

Location	Facilities
Physical Assembly Point	No physical area required
Virtual Assembly Point	Microsoft Teams will be used.

6.0 Incident Response Team

A well-coordinated incident response team is the lifeline to a successful recovery after a cyber security incident. Every member of the team has specific roles and responsibilities which must be carefully executed

when handling an incident. The main goal of this team is to minimise impact and restore normal operations as soon as possible.

The school's Incident Management Team will comprise the staff below:

Incident Response Role	Name	Role in school	Organisation	Mobile Phone
Incident Response Manager	Claire Bramley	Principal	Learning4Life-gy	07984129201
Business/Operations Manager	Sara Morris	CEO	Learning4Life-gy	07773559596
Technical Lead	Steve	Contractor	DBS Group	07942800813
Data Protection Officer	Louis Meller	ICT Teacher	Learning4Life-gy	07427894108

6.1 Roles and Responsibilities

When dealing with a cyber security incident, it's imperative to have a clear and concise layout of the responsibilities assigned to each member in the incident response team, for clarity and accountability.

Role	Responsibilities
Incident Response Manager	Coordinates the overall response activities and organises the resources required.
Senior Leadership Team / Senior Management Team	Making and documenting decisions at every stage of the response and recovery process, updating the board on progress, and handling media enquiries.
Learning4life-gy Business Manager	Coordinates resources, insurers, and legal guidance.
Technical Lead	Coordinates the core technical response; identifies internal or external parties with the required skills and expertise.
Data Protection Officer	Coordinates the cyber security incident response plan with the school's data protection processes, such as performing a Data Protection Impact Assessment or notifying the Information Commissioner's Office (ICO).

6.2 Tabletop Exercises

Conducting cyber incident response exercises is a good way of identifying gaps within the response process and preparing the incident response team. When performing exercises, the Learning4life-gy consults external expertise or tools using the Secure Schools Incident Response Simulator/NCSC's *Exercise In a Box*. The aim is to conduct exercises using a variety of scenarios and to document every step of the response process, then discuss any lessons learnt.

7.0 Incident Response Procedure

The incident response flow shows the significant processes and procedures that need to be implemented from when an incident is detected to when it's resolved.

- After the IT team detects or is notified of an incident, they immediately work to verify if the reported incident is genuine. If genuine, this should be recorded in the initial incident summary form.
- An impact assessment is carried out to verify the severity of the incident. If the impact is significant enough to trigger an incident response strategy, the incident response manager is notified. Some of the questions addressed at this stage are:
    - Are any critical business systems involved?
    - What could the severity of the potential impact be?
    - What are the details of the targeted systems?
    - Where is the source of the attack?
- The incident response manager collects factual information about the incident and assembles the incident management team. Some of the questions addressed at this stage are:
    - What are the initial findings?
    - What kind of incident is this (e.g., ransomware, denial of service, virus, physical damage, etc.)?
    - What kind of data or systems are being targeted?
    - Does the incident threaten school closure?
    - Has the incident been contained?
    - Does the school need to notify any external parties for legal reasons?
- If the breach involves the theft of personal information, affected individuals must be notified as soon as possible.

- The technical lead assembles a technical team and coordinates the overall technical response, and follows the technical incident response procedure to analyse, contain, eradicate and recover from the incident.
- If deemed necessary by the incident response team, relevant external parties and authorities are notified. The Data Protection Officer is responsible for performing an impact and risk assessment to establish if the incident should be reported to the Information Commissioner's Office. The Learning4life-gy may have to notify the police to proceed with any criminal convictions.
- When the incident is resolved, all the lessons learnt throughout the response process must be well documented in the **Post-incident Review Form** and all security recommendations must be incorporated into the Risk Action Plan. Some of the questions to be addressed to include in the review are:
    - How effective was the response?
    - Are there any changes that could make the response better?
    - Are there any changes to policies or additional policies needed?
    - What could have prevented the incident?
    - What were the changes made to ensure the incident is not repeated?
    - What were the lessons learnt?

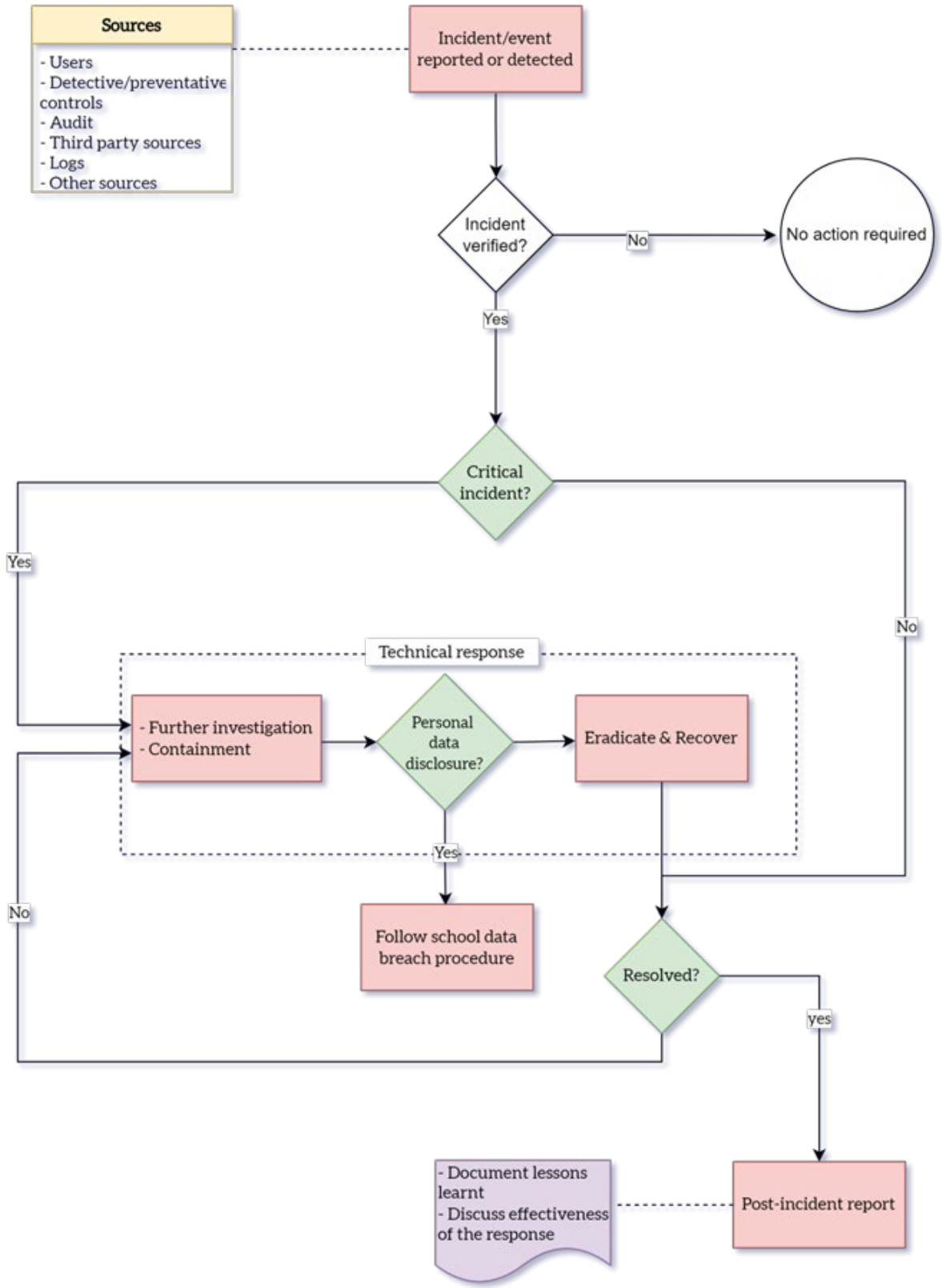

Fig 1: Incident response flow

7.1 Core Technical Response

The four main stages of a technical response are Analyse, Contain, Eradicate and Recover.

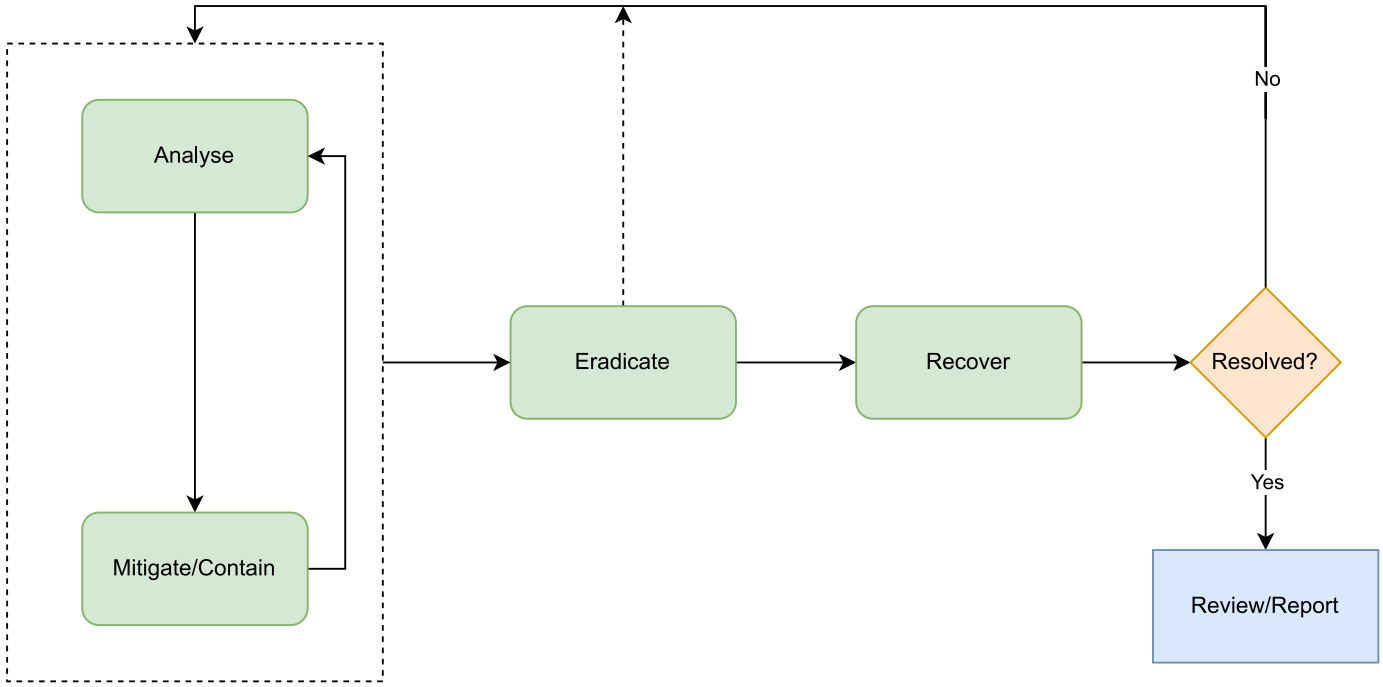

Fig 2: High-level technical response process

Analyse

Analysis is the first stage of the technical response process, and at this stage, the technical team uses both automated and manual techniques and tools to establish whether a system has been breached. This process will also identify the extent of damage caused and devices or accounts affected. As prompted in the Initial Incident Summary, they must document the source of the breach, method of discovery, time and date, impact, affected areas and operations, and whether the risk had already been identified according to the Learning4Life-gy's cyber risk register.

Containment and Eradication

The technical team will isolate the affected device(s) or account(s) from the rest of the network infrastructure. This precautionary measure stops the infection from spreading to other parts of a network. The device's connection to the internet will be removed by either removing the network cable or disabling the Wi-fi adapter. The vulnerability leading to the incident must be found and remediated. Once isolated, system updates, patches, and credential changes must be applied to the affected device(s) and the rest of the infrastructure.

Recovery

Once all vulnerabilities have been patched, and the system(s) are confirmed free from malware, the recovery process can begin. The affected computer systems can be restored from a fresh installation or a trusted backup and then incorporated into the operational network.

Reporting

After a successful recovery, it's essential to discuss the lessons learnt throughout the incident response. All the details of the incident will be well-documented alongside all the necessary improvements that need to be implemented. This is achieved through recommendations from the technical team being raised in a Risk Action Plan to avoid future incidents of the same nature.

8.0 Detection and Notification

All system users are responsible for notifying responsible staff when abnormal or unusual activity is detected. Any potential cyber security incident must be immediately reported to the IT support team, who will assess all events and escalate where appropriate. This notification process is included in Learning4Life-gy's IT Acceptable Use Policy accepted by all staff and is included in annual staff cyber security awareness training via CPD Training.

Sources of incident reports typically include:

- School Staff: reports of suspicious system activity, emails, strange human behaviour, unusual phone calls, etc.
- Technical: includes alerts from monitoring tools such as intrusion detection and prevention systems, anti-virus and SIEM solutions
- Third parties: reports from threat research or offensive security organisations, police, government agencies, suppliers, and partners.

8.1 Key Internal Contacts

Role in Learning4life-gy	Name and Department	Mobile Phone
Principal	Clare Bramley	07984129201
CEO/Director	Sara Morris	07773559596

IT Lead	Louis Meller	07427894108
Data Protection Officer	Louis Meller	07427894108
Safeguarding officer	Gwyn Little	01472 240440

8.2 Key External Contacts

Authorities

Organisation	Key Contact Name & Department	Work Phone	Mobile Phone
Local law enforcement	Humberside Police	101	101
Local authority (if applicable)	ICO / North East Lincs	0303 123 1113	

Suppliers

Supplier	Key Contact Name & Department	Account Number	Telephone Number
Internet service provider	**Matthew Dickel** Virgin Media	921517301	07977180187
Website host	Ionos	74788894	0333 336 5691

Appendices

Appendix (a): Initial Incident Summary Report Form

To be completed by the IT Lead.

Initial Incident Summary Report Form
Incident description
Date and time of detection
Source of detection
Detection method
Details of affected Systems/Segments (*including accounts and data*)
Source of breach (*if known*)

Appendix (b): Decision/Action Log

To be completed by Senior Leadership Team member.

Date/Time	Decision/Action	Responsible Person

Appendix (c): Post-incident Review Form

To be completed by the Incident Response Manager and IT Lead.

Post-incident Review Form	
Date incident resolved	
Incident response plan comments	
Improvements to the incident response plan	
Incident Type	
Incident Cause	
Affected Systems	

Incident details

Actions taken

Lessons learnt

Recommendations

Created by	Louis Meller
Date	12/10/2022
Date of Next Review	12/10/2023

Date	Changes	Signed
12/02/24	Added revision table to end of policy	Louis Meller