THE BAY
LEARNING TRUST

Cyber Incident Response Process

The Bay Learning Trust
The Lodge
Ripley St Thomas
Ashton Road
Lancaster
LA1 4RR

t 01524 581872
e admin@baylearningtrust.com
website baylearningtrust.com

Document Control

This document has been approved for operation within:	**All Trust Establishments**
Date effective from	**September 2023**
Date of next review	**September 2024**
Review period	**12 months**
Status	**Statutory**
Owner	**The Bay Learning Trust**
Version	**v1.0**

The Bay Learning Trust Cyber Incident Response Process

Contents

1. Statement of Intent

1.1 The Bay Learning Trust is committed to maintaining the confidentiality, integrity and availability of its information and continuity of business, teaching and learning throughout the Trust's Academies.

The Bay Learning Trust recognises, however, that breaches in security and cyber-incidents can occur. This plan is to document process and assist in dealing with cyber-incidents.

This policy has due regard to the academies policies and procedures including, but not limited to, the following:

- Cyber Incident Response and Recovery Plan
- Cyber Security Policy

2. Key Contacts

2.1

- Sally Kenyon - CEO
- Sue Farrimond – Deputy CEO
- Andrew McKinnell – Chief Operating Officer / Chief Finance Officer
- Gavin Gomersall - DPO
- Ian Jones – Trust ICT Manager

3. Severity Matrix

3.1 Critical

- Over 80% of staff/Pupils (or several critical staff/teams) unable to work
- Critical systems offline with no known resolution
- High risk to / definite breach of sensitive client or personal data
- Severe Financial impact
- Severe reputational damage

3.2 High

- 50% of staff/pupils unable to work
- Risk of breach of personal or sensitive data
- Non-critical systems affected, or critical systems affected with known (quick) resolution
- High Financial impact
- Potential serious reputational damage

3.3 Medium

- 20% of staff/Pupils unable to work
- Possible breach of small amounts of non-sensitive data
- Low risk to reputation
- Small number of non-critical systems affected with known resolutions

3.4 Low

- Minimal, if any, impact
- One or two non-sensitive / non-critical machines affected
- <10% of staff/Pupils affected temporarily (short term)

4. Incident Category

- **Malicious code -** Malware infection on the network, including ransomware
- **Denial of Service -** Typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
- **Phishing -** Emails attempting to convince someone to trust a link/attachment.
- **Unauthorised Access -** Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account.
- **Insider -** Malicious or accidental action by an employee or pupil causing a security incident.
- **Data breach -** Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
- **Targeted attack -** An attack specifically targeted at the school - usually by a sophisticated attacker (often encompassing several of the above categories).

5. Core Response

- **Analyse** – Determine the category of the incident and review necessary steps to contain and mitigate the threat
- **Contain/Mitigate** – Take steps to reduce the impact of the incident and prevent things from getting worse. E.g. Taking systems offline disconnecting from network etc
- **Remediate/Eradicate** – fully remove threat from the network and systems. E.g. clean virus or malicious code
- **Recover** – Restore systems to previous state and resume normal operating processes.

6. Post Incident Review

- Are there security improvements which could have prevented the incident, or enabled earlier detection?
- Consider both the tactical fixes that would have prevented or detected this incident as well as strategic solutions that may only be identifiable across multiple incidents. For example, ineffective governance processes leading to multiple intrusions through previously un-recorded, internet-facing, assets.
- In particular, was there any information which would have significantly helped your response but which was difficult or impossible to obtain?
- Was the response successful and effective?
- Were there elements which could have been handled better?
- Was there data which could have been useful but wasn't available (For example, the right logs, or something that was overwritten early in the response?). *Keeping a record of activities during the response will assist with this review.*
- Were the relevant data and tools available to enable the analysis?
- Did the processes and communications work well?
- Were the right people involved and empowered to make the necessary decisions?