# CONNECTED LEARNING
# SECURITY INCIDENTS POLICY

| Document Detail | |
|---|---|
| **Category:** | Information Governance |
| **Authorised By:** | CL Board of Trustees |
| **Status:** | APPROVED |
| **Date Approved:** | 21.10.20 |
| **Next Review Date:** | Annually – October 2021 |

# Security Incidents Policy

A security incident is a confirmed breach, potential breach or ‘near-miss’ breach of one of CL’s information policies

**What must I do? Why must I do it? How must I do it?**

1. ***MUST***: If you discover a security incident, you must immediately **report** it to the Information Champion (details below).
   Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective
   Please notify the Information Champion immediately. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible. In the event that a security incident is detected out of hours, the Head of School must be alerted. (S)he must then contact the Information Champion at the earliest opportunity.

2. ***MUST***: When reporting the incident, you must **provide** as much information as possible
   To help us quickly assess the severity of the incident and to speed up the investigation
   Include full details of the incident such as dates, names and any remedial action that has been taken

3. ***MUST***: The Information Champion must **complete** investigations and complete an outcome report
   Carry out an effective process appropriate to the severity of the incident
   Where appropriate, undertake the following:
   a. Identify expected outcomes, stakeholders and any policies breached.
   b. Speak to staff involved.
   c. Record evidence and keep an audit trail of events and evidence supporting decisions taken
   d. Get expert help

e. Escalate
f. Inform data subjects (service users, staff) where appropriate
g. Identify and manage risks of the incident
h. Commence disciplinary action, or record why not
i. Develop and implement a communications plan where appropriate
j. Put in place controls to prevent recurrence
k. Complete the Incident Outcome Report

4. ***MUST***: All staff must support investigations into incidents as required
Carry out an effective process appropriate to the severity of the incident
a. Where appropriate, undertake the following:
b. Work with the SIRO to investigate major security incidents.
c. Assess the outcome to ensure the appropriate action has been taken.
d. Provide knowledge and advice, and carry out any recommended actions for major or critical incidents, where require

5. ***MUST*:** Maintain a full **record** of each incident from reporting to closure
Ensure the process if followed to completion
a. Classify the Security Incident
b. Verify the details and oversee the investigation
c. Work with SIRO to investigate major security incidents.
d. Advise, support and intervene as appropriate
e. Review Incident Outcome Reports and close

***6.*** ***MUST***: The Information Champion & SIRO must support the investigation of **major and critical** incidents
Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents
Undertake the following:
For major and critical incidents:
a. Undertake the investigation (critical only)
b. Work with [insert role(s)/ team(s)] (major only)
c. Assess if it is necessary for the security incident to be reported to the ICO.
d. Complete an outcome report and recommend remedial actions

***7.*** ***MUST***: Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident
Ensure that all incidents are handled in a timely manner.
Follow the process outlined in the Trust's Procedures for Reporting or Handling a Security Incident

8. ***MUST:*** *Major* and critical incidents must be referred to the Data Protection Officer.
Ensure that serious incidents are reviewed against the criteria for reporting to the regulator

## What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the Information Champion.

If you believe the policy does not meet your business needs, you may raise this with your Information Champion who, if they agree with your suggestion, may propose a policy change.

## Document Control

| | | |
|---|---|---|
| Version: | 3 | TRUST INFORMATION CHAMPION |
| Date approved: | | Tina Weavers |
| Approved by: | Board of Trustees | tinaweavers@connectedlearningmat.co.uk |
| Next review: | Annually - May 2020 | 01376 518190 |

## References

- Data Protection Act 2018

## Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.